Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 92045

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

SecurityProfiling, LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/Thomas D. Fortenberry/	Date (Optional)	
Name	Thomas D. Fortenberry		
Title	Manager of SecurityProfiling, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

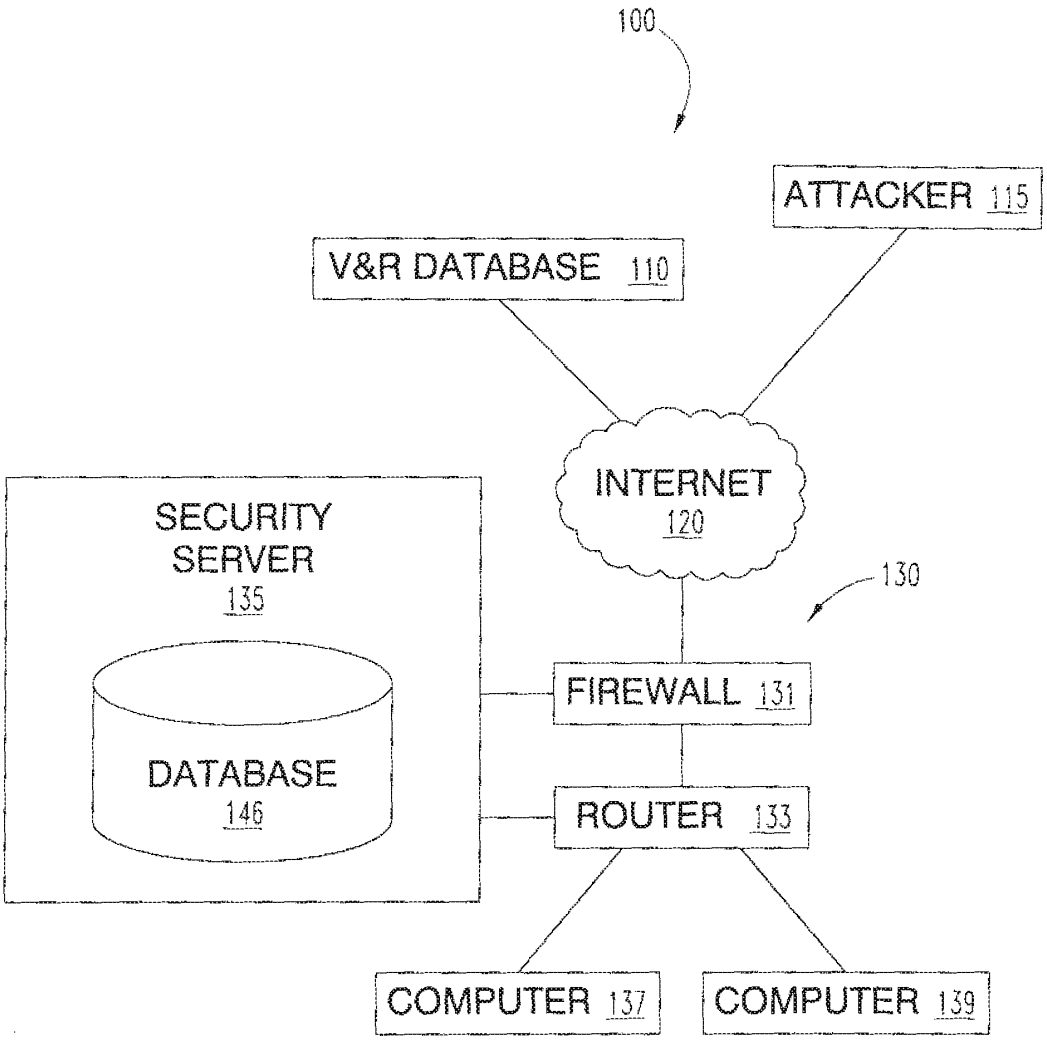

100
ATTACKER 115
V&R DATABASE 110
INTERNET 120
SECURITY SERVER 135
DATABASE 146
130
FIREWALL 131
ROUTER 133
COMPUTER 137
COMPUTER 139

FIG. 1

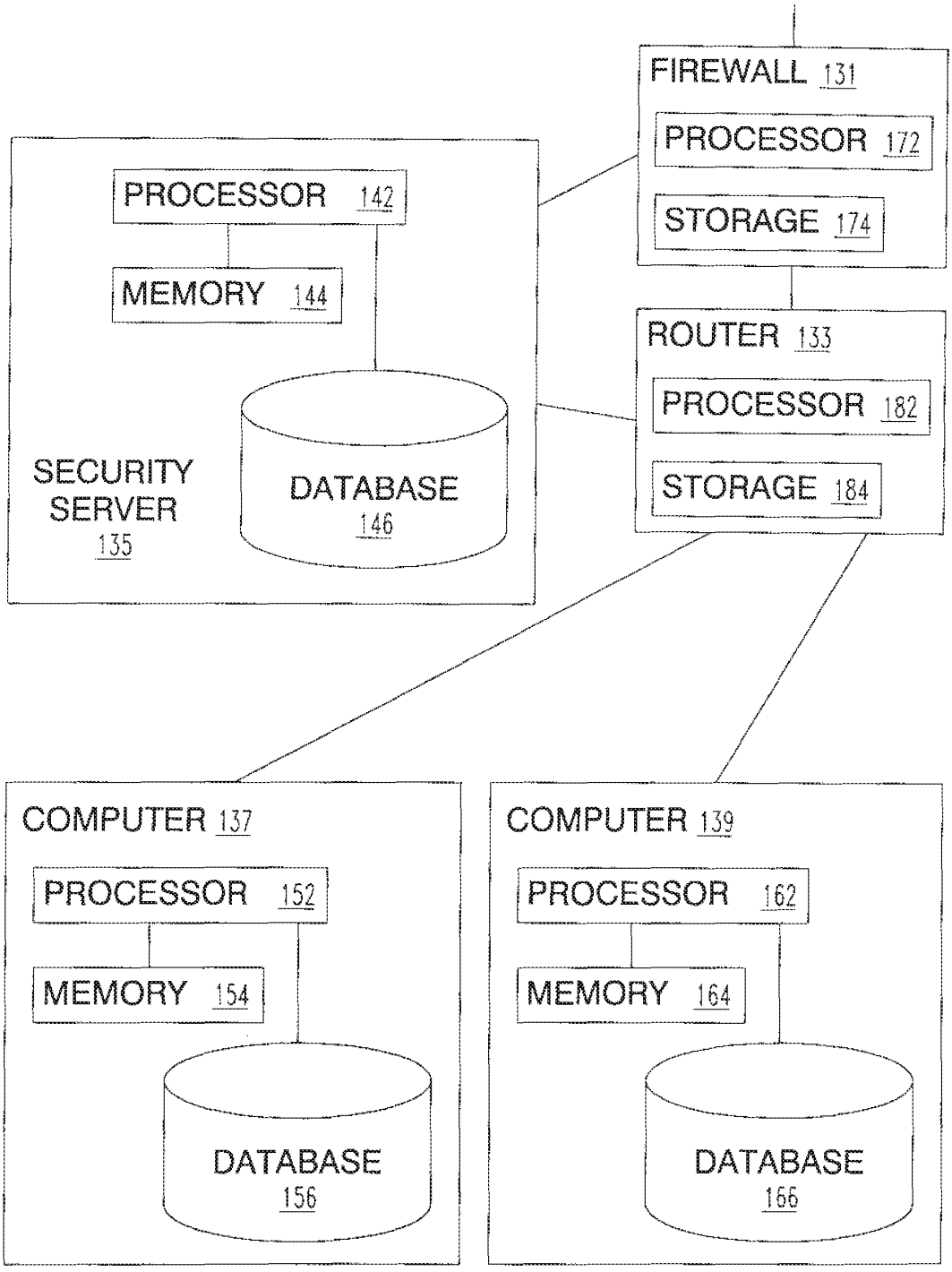

FIREWALL 131
PROCESSOR 172
STORAGE 174
PROCESSOR 142
MEMORY 144
ROUTER 133
PROCESSOR 182
STORAGE 184
SECURITY SERVER 135
DATABASE 146
COMPUTER 137
PROCESSOR 152
MEMORY 154
DATABASE 156
COMPUTER 139
PROCESSOR 162
MEMORY 164
DATABASE 166

FIG. 2

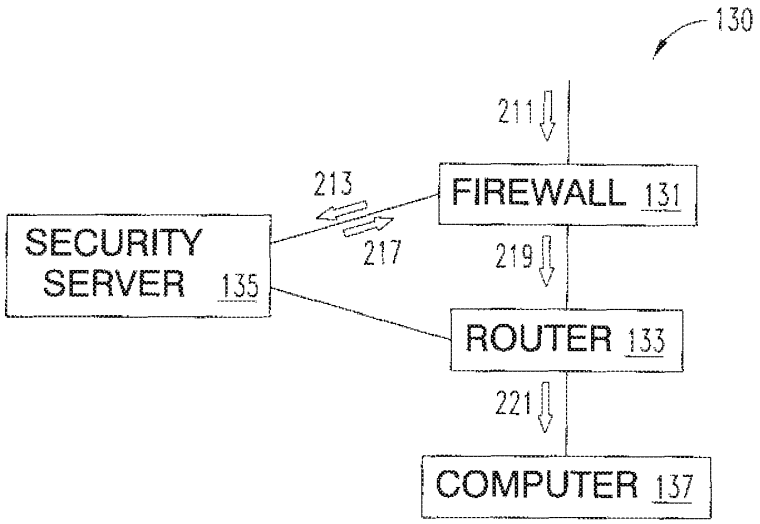

130
211
FIREWALL 131
213
217
SECURITY SERVER 135
219
ROUTER 133
221
COMPUTER 137

FIG. 3

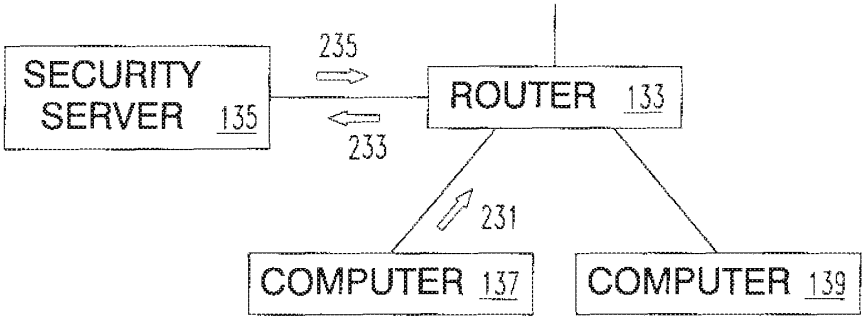

235
SECURITY SERVER 135
ROUTER 133
233
231
COMPUTER 137
COMPUTER 139

FIG. 4

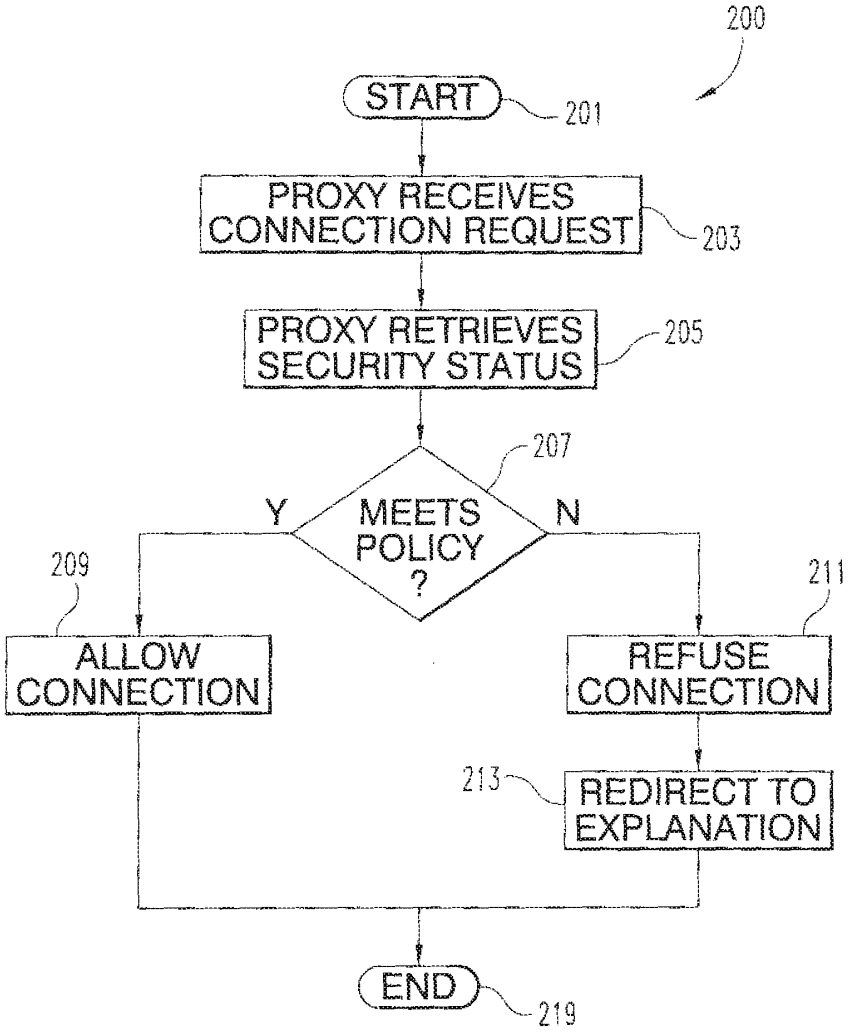

200
START
201
PROXY RECEIVES CONNECTION REQUEST
203
PROXY RETRIEVES SECURITY STATUS
205
207
MEETS POLICY ?
Y
N
209
ALLOW CONNECTION
211
REFUSE CONNECTION
213
REDIRECT TO EXPLANATION
END
219

FIG. 5A

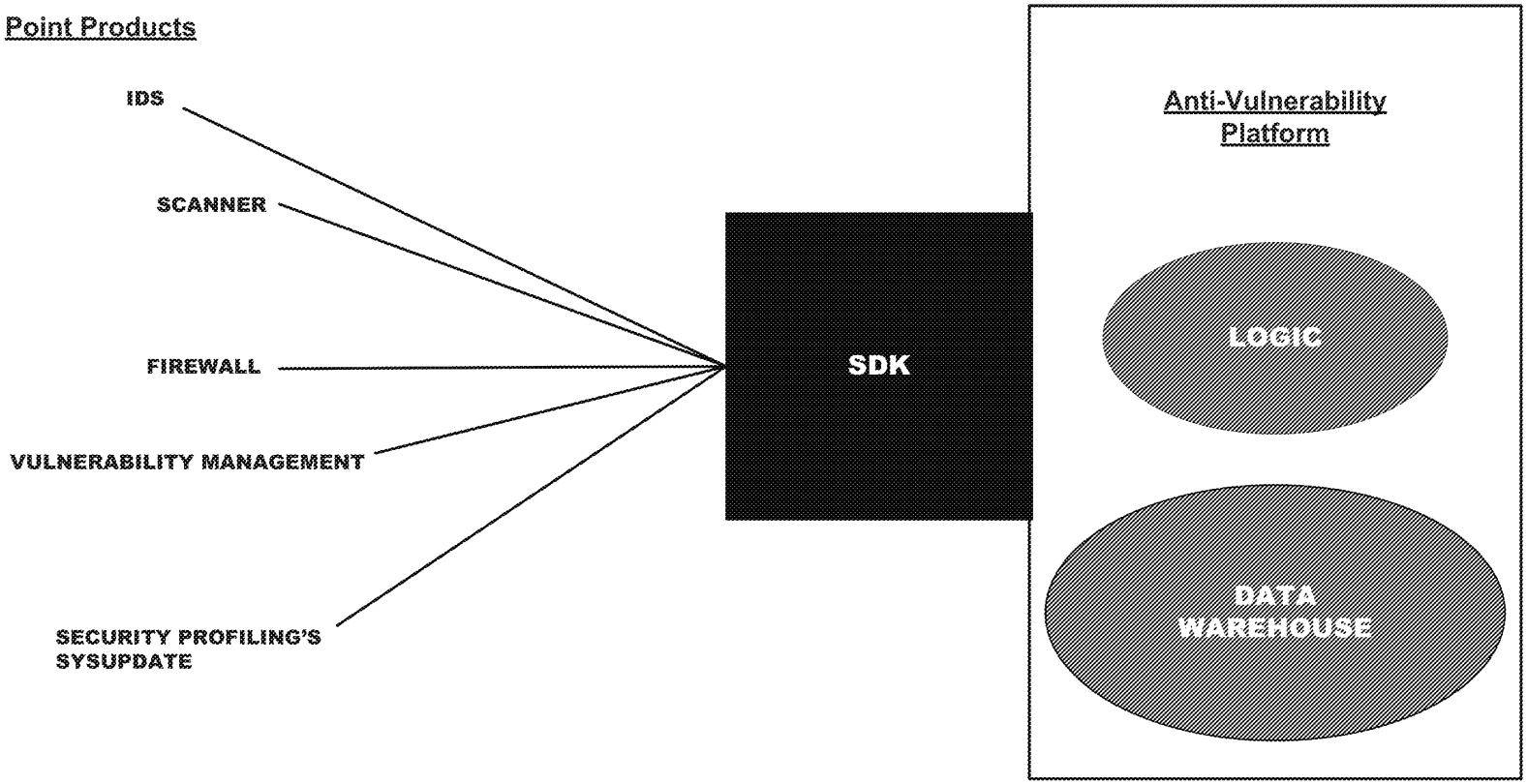


FIG. 5B

ForcePoint LLC
EX-1002
Page006

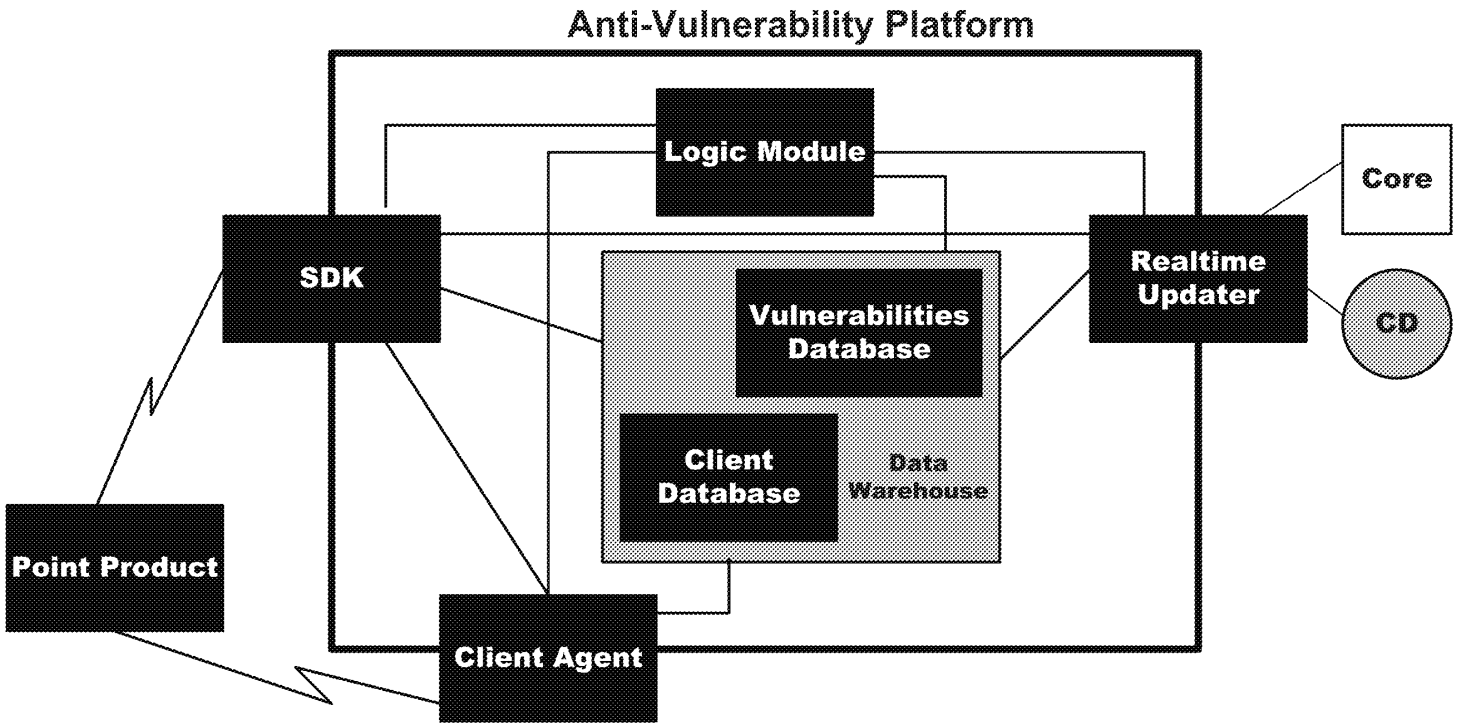


FIG. 6

ForcePoint LLC
EX-1002
Page007

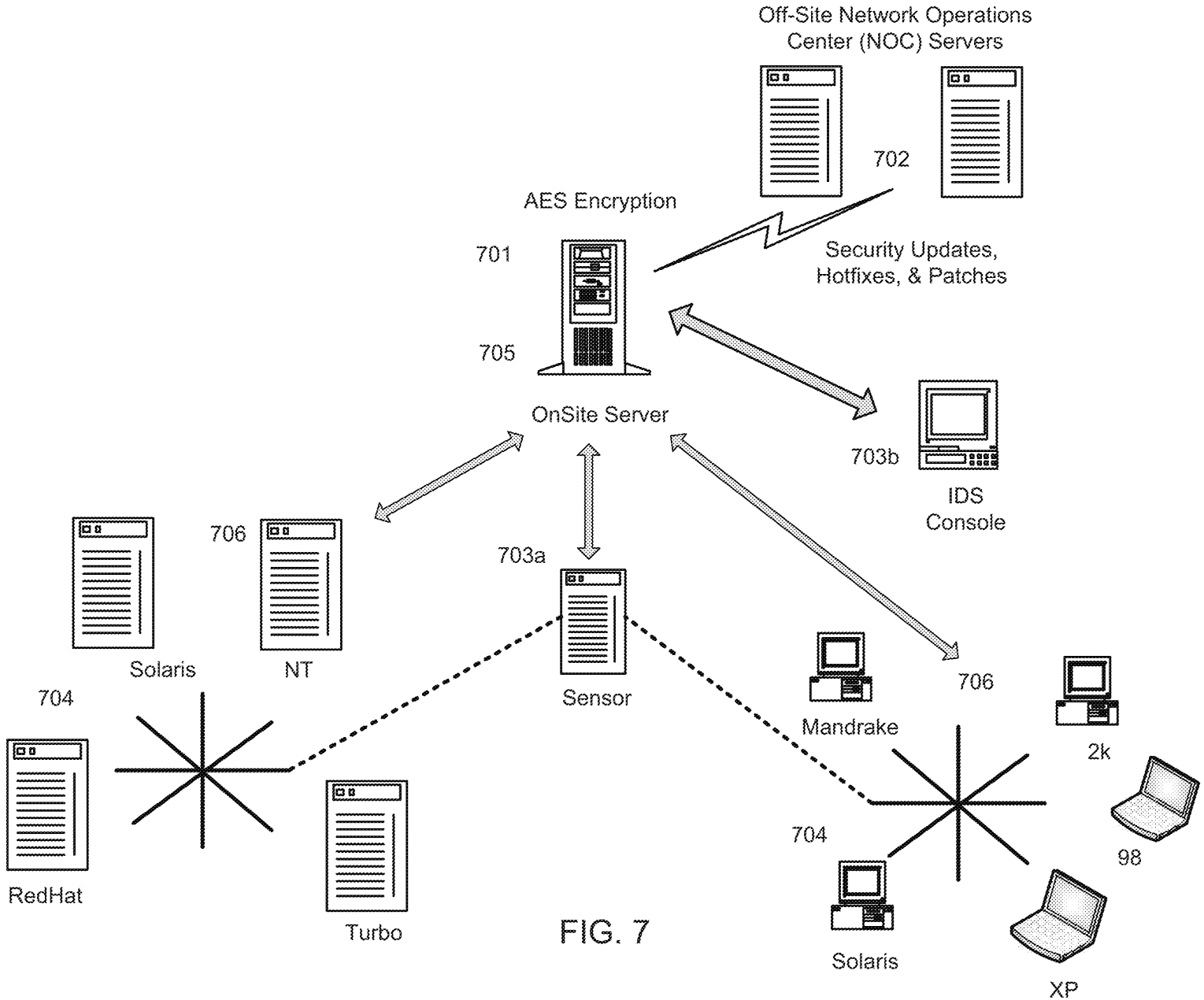


FIG. 7

ForcePoint LLC
EX-1002
Page008

Network Operations Center
(NOC) Servers
802
Security Updates,
Hotfixes, & Patches
803
Management
Console(s)
801
805
OnSite Server
AES Encryption
Group One
Group Two
806
NT
Turbo
2k
Solaris
RedHat
804
806
2k
98
XP
Solaris
804
2k

FIG. 8

901
LogBoss™
On-Site Server
903
904
Viewer
Console
Scaleable to Any Size or Architecture
Group One
Group Two
902
Web Server
E-Mail Server
Data Storage Server
Database Server
File Server
902
Workstation
Workstation
Laptop
Laptop
Workstation

FIG. 9

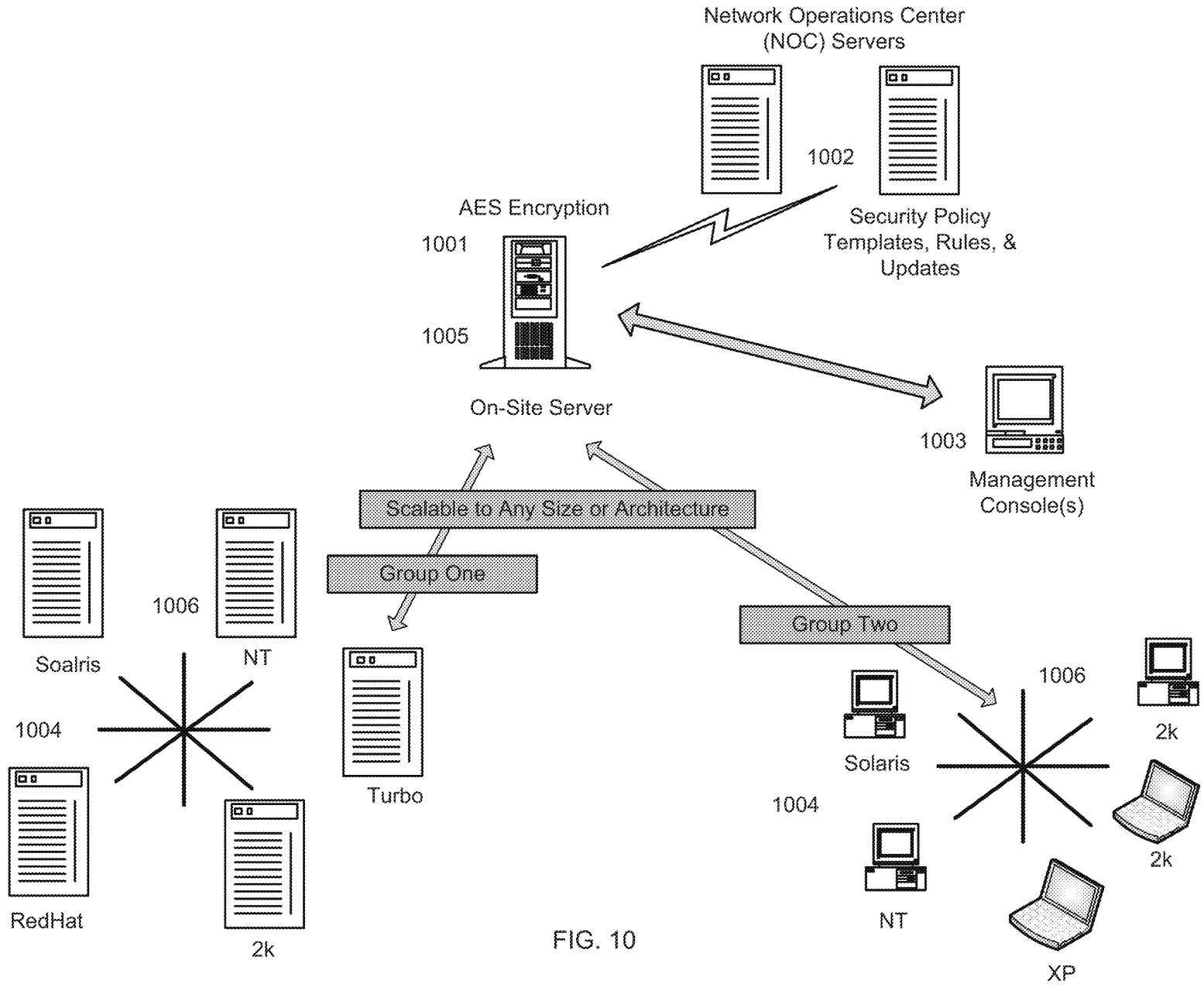


FIG. 10

ForcePoint LLC
EX-1002
Page011

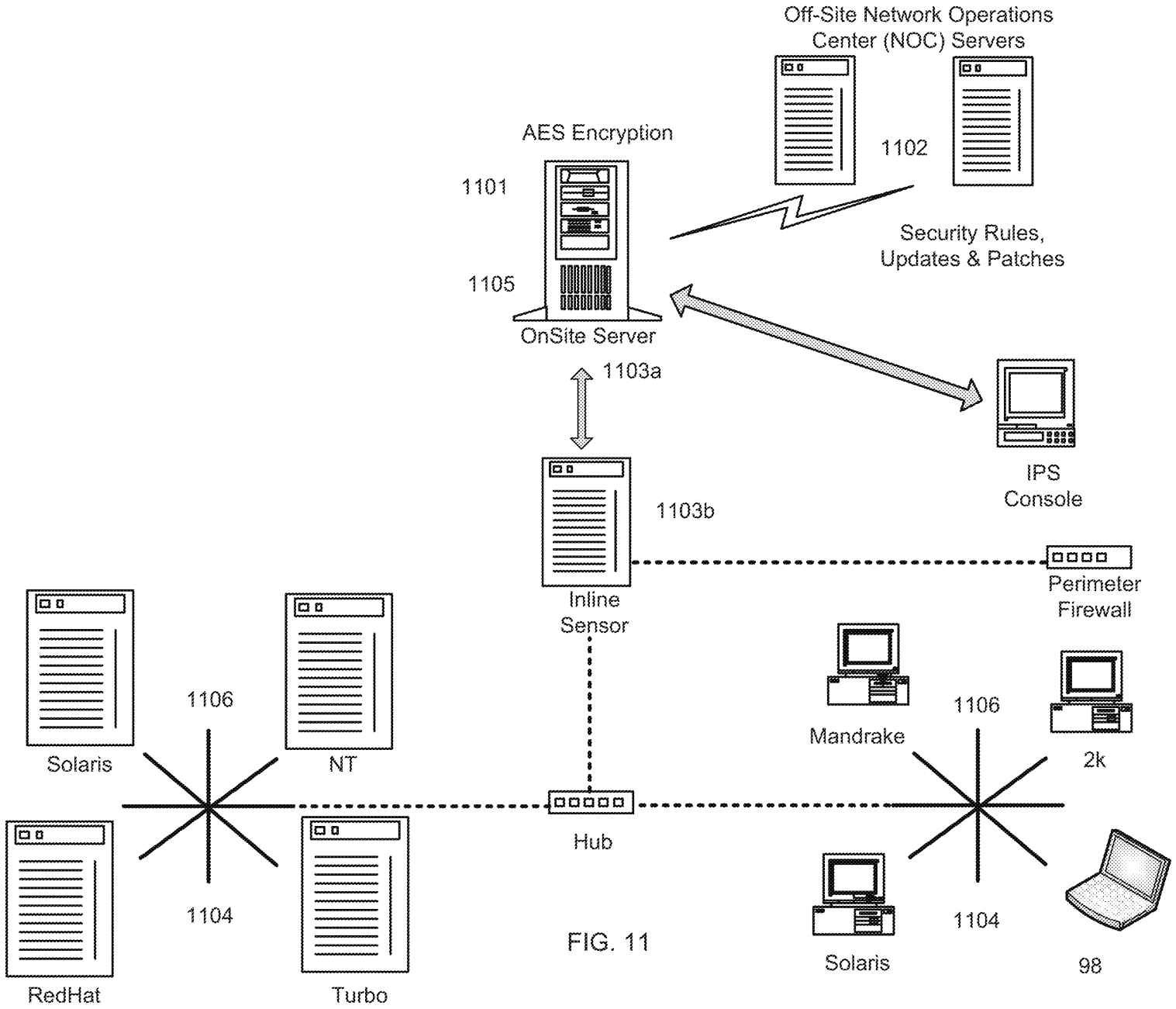


FIG. 11

ForcePoint LLC
EX-1002
Page012

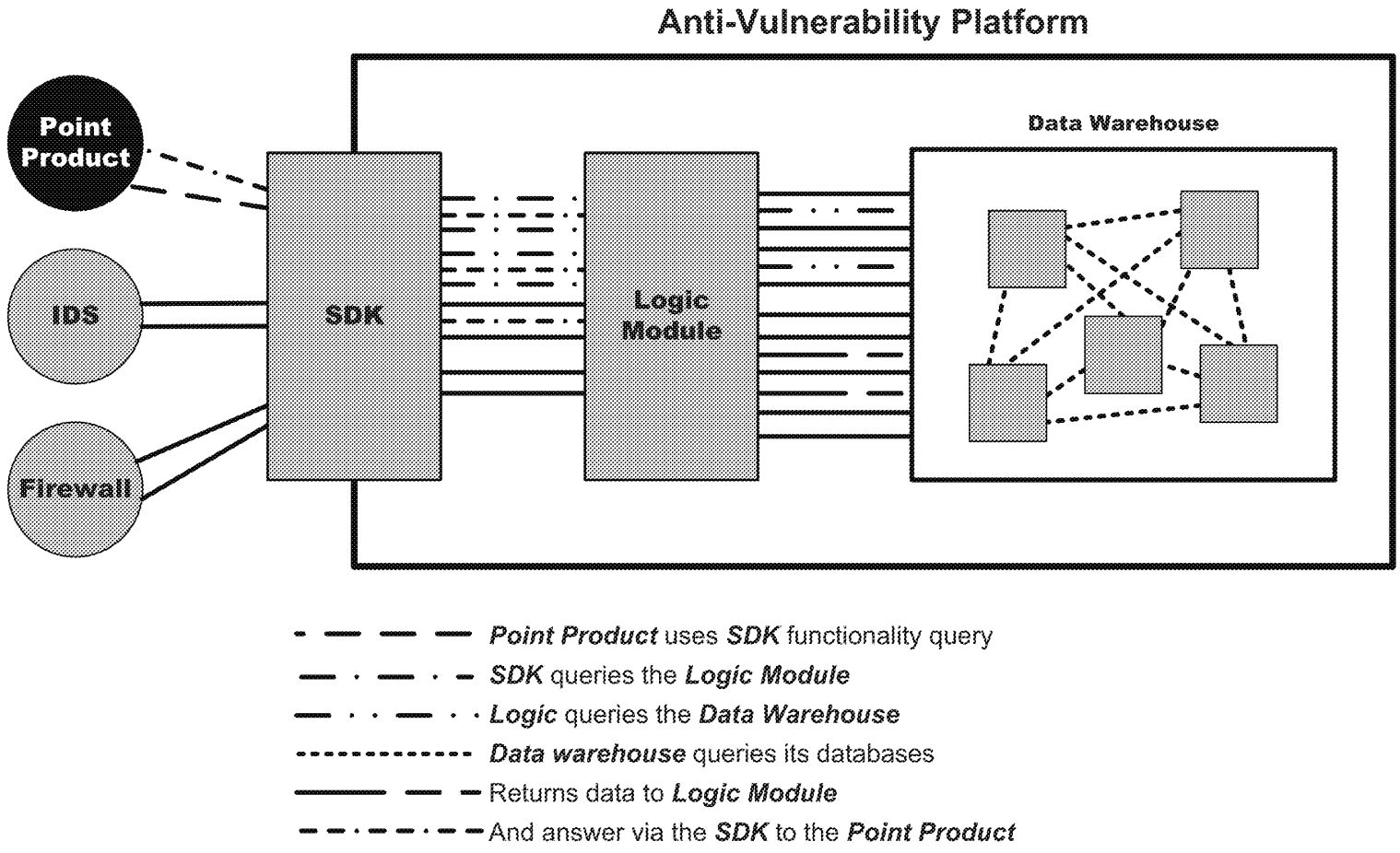


FIG. 12

ForcePoint LLC
EX-1002
Page013

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of, and claims priority to, U.S. App. No.: 14/816,931, filed August 3, 2015, which, in turn, is a continuation of U.S. App. No.: 14/499,230, now U.S. Pat. No.: 9,100,431, filed September 28, 2014 which, in turn, is a continuation-in-part of U.S. App. No.: 14/138,014 filed December 21, 2013, now U.S. Pat. No.: 9,117,069, which, in turn, is a continuation of U.S. App. No.: 10/882,852 filed July 1, 2004 which, in turn, claims priority to U.S. App. No.: 60/484,085 filed July 1, 2003, which are all incorporated herein by reference in their entirety for all purposes.

FIELD OF THE INVENTION

[0002] The present invention relates to computer systems, and more particularly to management of security of computing and network devices that are connected to other such devices.

SUMMARY

[0003] A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration

ForcePoint LLC
EX-1002
Page014

option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a block diagram of a networked system of computers in one embodiment of the present invention.

[0005] FIG. 2 is a block diagram showing components of several computing devices in the system of FIG. 1.

[0006] FIGS. 3 and 4 trace signals that travel through the system of FIGS. 1 and 2 and the present invention is applied to them.

[0007] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0008] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0009] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment.

[0010] FIG. 8 illustrates an update system, in accordance with one embodiment.

[0011] FIG. 9 shows a configured network, in accordance with one embodiment.

[0012] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[0013] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[0014] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

DETAILED DESCRIPTION

GLOSSARY

ForcePoint LLC
EX-1002
Page015

[0015] data warehouse = a component that contains vulnerabilities and updates for devices that operate on at least one network

[0016] NOC server = network operations center server that periodically synchronize latest vulnerability and update data with other servers.

[0017] SDK = software development kit that allows programmers to develop security applications that access data collected in a database

[0018] CM application = change management application that controls documentation and logging of change.

[0019] For the purpose of promoting an understanding of the principles of the present invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will, nevertheless, be understood that no limitation of the scope of the invention is thereby intended; any alterations and further modifications of the described or illustrated embodiments, and any further applications of the principles of the invention as illustrated therein are contemplated as would normally occur to one skilled in the art to which the invention relates.

[0020] Generally, the present invention in one embodiment operates in the context of a network as shown in FIG. 1. System 100 includes a vulnerability and remediation database 110 connected by Internet 120 to subnet 130. In this exemplary embodiment, firewall 131 serves as the gateway between Internet 120 and the rest of subnet 130. Router 133 directs connections between computers 137 and each other and other devices on Internet 120. Server 135 collects certain information and provides certain data services that will be discussed in further detail herein.

[0021] In particular, security server 135 includes processor 142, and memory 144 encoded with programming instructions executable by processor 142 to perform several important security-related functions. For example, security server 135 collects data from devices 131, 133, 137, and 139, including the software installed on those devices, their configuration and policy settings, and patches that have been installed. Security server 135 also obtains from vulnerability and remediation database 110 a regularly updated list of security vulnerabilities in software for a

ForcePoint LLC
EX-1002
Page016

wide variety of operating systems, and even in the operating systems themselves. Security server 135 also downloads a regularly updated list of remediation techniques that can be applied to protect a device from damage due to those vulnerabilities. In one embodiment, each vulnerability in remediation database 110 is identified by a vulnerability identifier, and the vulnerability identifier can be used to retrieve remediation information from database 110 (and from database 146, discussed below in relation to FIG. 2).

[0022] In one embodiment, computers 137 and 139 each comprise a processor 152, 162, memory 154, 164, and storage 156, 166. Computer 137 executes a client-side program (stored in storage 156, loaded into memory 154, and executed by processor 152) that maintains an up-to-date collection of information regarding the operating system, service pack (if applicable), software, and patches installed on computer 137, and the policies and configuration data (including configuration files, and elements that may be contained in files, such as *.ini and *.conf files and registry information, for example), and communicates that information on a substantially real-time basis to security server 135. In an alternative embodiment, the collection of information is not retained on computer 137, but is only communicated once to security server 135, then is updated in real time as changes to that collection occur.

[0023] Computer 139 stores, loads, and executes a similar software program that communicates configuration information pertaining to computer 139 to security server 135, also substantially in real time. Changes to the configuration registry in computer 139 are monitored, and selected changes are communicated to security server 135 so that relevant information is always available. Security server 135 may connect directly to and request software installation status and configuration information from firewall 131 and router 133, for embodiments wherein firewall 131 and router 133 do not have a software program executing on them to communicate this information directly.

[0024] This collection of information is made available at security server 135, and combined with the vulnerability and remediation data from source 110. The advanced functionality of system 100 is thereby enabled as discussed further herein.

[0025] Turning to FIG. 2, one sees additional details and components of the devices in subnet 130. Computers 137 and 139 are traditional client or server machines, each having a processor 152, 162, memory 154, 164, and storage 156, 166. Firewall 131 and router 133 also

ForcePoint LLC
EX-1002
Page017

have processors 172, 182 and storage 174, 184, respectively, as is known in the art. In this embodiment, devices 137 and 139 each execute a client-side program that continuously monitors the software installation and configuration status for that device. Changes to that status are communicated in substantially real time to security server 135, which continuously maintains the information in database 146. Security server 135 connects directly to firewall 131 and router 133 to obtain software installation and configuration status for those devices in the absence of a client-side program running thereon.

[0026] Processors 142, 152, 162 may each be comprised of one or more components configured as a single unit. Alternatively, when of a multi-component form, processor 142, 152, 162 may each have one or more components located remotely relative to the others. One or more components of processor 142, 152, 162 may be of the electronic variety defining digital circuitry, analog circuitry, or both. In one embodiment, processor 142, 152, 162 are of a conventional, integrated circuit microprocessor arrangement, such as one or more PENTIUM 4 or XEON processors from INTEL Corporation of 2200 Mission College Boulevard, Santa Clara, Calif., 95052, USA, or ATHLON XP processors from Advanced Micro Devices, One AMD Place, Sunnyvale, Calif., 94088, USA.

[0027] Memories 144, 154, 164 may include one or more types of solid-state electronic memory, magnetic memory, or optical memory, just to name a few. By way of non-limiting example, memory 40b may include solid-state electronic Random Access Memory (RAM), Sequentially Accessible Memory (SAM) (such as the First-In, First-Out (FIFO) variety or the Last-In First-Out (LIFO) variety), Programmable Read Only Memory (PROM), Electrically Programmable Read Only Memory (EPROM), or Electrically Erasable Programmable Read Only Memory (EEPROM); an optical disc memory (such as a DVD or CD ROM); a magnetically encoded hard drive, floppy disk, tape, or cartridge media; or a combination of any of these memory types. Also, memories 144, 154, 164 may be volatile, nonvolatile, or a hybrid combination of volatile and nonvolatile varieties.

[0028] In this exemplary embodiment, storage 146, 156, 166 comprises one or more of the memory types just given for memories 144, 154, 164, preferably selected from the non-volatile types.

ForcePoint LLC
EX-1002
Page018

[0029] This collection of information is used by system 100 in a wide variety of ways. With reference to FIG. 3, assume for example that a connection request 211 arrives at firewall 131 requesting that data be transferred to computer 137. The payload of request 211 is, in this example, a probe request for a worm that takes advantage of a particular security vulnerability in a certain computer operating system. Based on characteristics of the connection request 211, firewall 131 sends a query 213 to security server 135. Query 213 includes information that security server 135 uses to determine (1) the intended destination of connection request 211, and (2) some characterization of the payload of connection request 211, such as a vulnerability identifier. Security server 135 uses this information to determine whether connection request 211 is attempting to take advantage of a particular known vulnerability of destination machine 137, and uses information from database 146 (see FIG. 2) to determine whether the destination computer 137 has the vulnerable software installed, and whether the vulnerability has been patched on computer 137, or whether computer 137 has been configured so as to be invulnerable to a particular attack.

[0030] Security server 135 sends result signal 217 back to firewall 131 with an indication of whether the connection request should be granted or rejected. If it is to be granted, firewall 131 passes the request to router 133 as request 219, and router 133 relays the request as request 221 to computer 137, as is understood in the art. If, on the other hand, signal 217 indicates that connection request 211 is to be rejected, firewall 133 drops or rejects the connection request 211 as is understood in the art.

[0031] Analogous operation can protect computers within subnet 130 from compromised devices within subnet 130 as well. For example, FIG. 4 illustrates subnet 130 with computer 137 compromised. Under the control of a virus or worm, for example, computer 137 sends connection attempt 231 to router 133 in an attempt to probe or take advantage of a potential vulnerability in computer 139. On receiving connection request 231, router 133 sends relevant information about request 231 in a query 233 to security server 135. Similarly to the operation discussed above in relation to FIG. 3, security server 135 determines whether connection request 231 poses any threat, and in particular any threat to software on computer 139. If so, security server 135 determines whether the vulnerability has been patched, and if not, it determines whether computer 139 has been otherwise configured to avoid damage due to that vulnerability.

ForcePoint LLC
EX-1002
Page019

Security server 135 replies with signal 235 to query 233 with that answer. Router 133 uses response 235 to determine whether to allow the connection attempt.

[0032] In some embodiments, upon a determination by security server 135 that a connection attempt or other attack has occurred against a computer that is vulnerable (based on its current software, patch, policy, and configuration status), security server 135 selects one or more remediation techniques from database 146 that remediate the particular vulnerability. Based on a prioritization previously selected by an administrator or the system designer, the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to the same vulnerability (based on their real-time software, patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied.

[0033] In various embodiments, remediation techniques include the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device's configuration; stopping, disabling, or removing services; setting or modifying policies; and the like. Furthermore, in various embodiments, events and actions are logged (preferably in a non-volatile medium) for later analysis and review by system administrators. In these embodiments, the log also stores information describing whether the target device was vulnerable to the attack.

[0034] A real-time status database according to the present invention has many other applications as well. In some embodiments, the database 146 is made available to an administrative console running on security server 135 or other administrative terminal. When a vulnerability is newly discovered in software that exists in subnet 130, administrators can immediately see whether any devices in subnet 130 are vulnerable to it, and if so, which ones. If a means of remediation of the vulnerability is known, the remediation can be selectively applied to only those devices subject to the vulnerability.

[0035] In some embodiments, the database 146 is integrated into another device, such as firewall 131 or router 133, or an individual device on the network. While some of these embodiments might avoid some failures due to network instability, they substantially increase the complexity of the device itself. For this reason, as well as the complexity of maintaining security database functions when integrated with other functions, the network-attached device embodiment described above in relation to FIGS. 1-4 is one possible embodiment.

ForcePoint LLC
EX-1002
Page020

[0036] In one embodiment, a software development kit (SDK) allows programmers to develop security applications that access the data collected in database 146. The applications developed with the SDK access information using a defined application programming interface (API) to retrieve vulnerability, remediation, and device status information available to the system. The applications then make security-related determinations and are enabled to take certain actions based on the available data.

[0037] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as, the Windows Registry on Microsoft WINDOWS operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0038] In one embodiment, security information management system is provided, wherein a database of potential vulnerabilities is maintained, along with data describing remediation techniques (patches, policy settings, and configuration options) available to protect against them. At least one vulnerability is associated in the database with multiple available remediation techniques. In one embodiment, the system presents a user with the list of remediation techniques available to protect against a known vulnerability, accepts the user's selection from the list, and executes the selected technique. In other embodiments, the system uses a predetermined prioritization schedule to automatically select among the available remediation techniques, then automatically executes the selected technique.

[0039] One embodiment of the present invention is a database of information about a plurality of devices, updated in real-time and used by an application to make a security-related decision. The database stores data indicating the installed operating system(s), installed software, patches that have been applied, system policies that are in place, and configuration information for each device. The database answers queries by one or more devices or applications attached by a network to facilitate security-related decision making. In one form of this embodiment, a firewall or router handles a connection request or maintenance of a connection based on the

ForcePoint LLC
EX-1002
Page021

configuration information stored in the database that relates to one or both of the devices involved in the transmission.

[0040] In one embodiment, database 146 includes vulnerability and remediation information such that, for at least one vulnerability, multiple methods of remediating the vulnerability are specified. When the system has occasion to implement or offer remediation of a vulnerability, all known alternatives are presented that are relevant to the device or machine's particular configuration or setup. For example, when a vulnerability of a device is presented to an administrator, the administrator is given a choice among the plurality of remediation options to remediate the vulnerability. In some embodiments, the administrator can select a preferred type of remediation that will be applied if available and a fallback type. For example, an administrator may select application of a policy setting over installation of a software patch, so that the risk of disruption of critical business systems is minimized.

[0041] In other embodiments, an administrator or other user is presented with a set of user interface elements that identify multiple options for remediating and identifying the vulnerability. The administrator or user selects the method to be used, and that remediation is applied to the vulnerable device(s).

[0042] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0043] In use, a database maintains security status information on each device in a network, based on whether the device's operating system, software, and patches are installed and configured to meet a baseline level of security. A network gateway proxy blocks connection attempts from devices for which the database indicates a substandard security status, but allows connections from other devices to pass normally. The database is preferably updated on a substantially real-time basis by client-side software run by each device in the network.

[0044] Another form of the present embodiment includes a connection proxy that filters connections originating within the network. In particular, one embodiment employs a proxy that denies connection attempts originating with devices in the network when the originating device has a status, reflected in the database, that fails to meet predetermined security characteristics in terms of installed operating system and software, patch levels, and system policy and configuration registry information.

ForcePoint LLC
EX-1002
Page022

[0045] In this embodiment, router 133 serves as a connection proxy for devices and subnet 130, as will be understood by those skilled in the art. In addition to basic proxy functionality, however, router 133 accesses database 146 on security server 135 via the SDK at each connection attempt. If, for example, device 137 attempts to connect to any device where the connection must pass through the proxy server (router 133 in this example), such as a device on Internet 120, router 133 checks the security status of device 137 in database 146, using the real-time status therein to determine whether device 137 complies with one or more predetermined security policies. If it does, router 133 allows the connection to be made. If it does not, router 133 prevents the connection, preferably redirecting the connection to a diagnostic page that explains why the connection is not being made.

[0046] This system is illustrated by method 200 in FIG. 5A. Method 200 begins with start point 201. The proxy (router 133 in the above example) receives a connection request at block 203, then retrieves the security status of the source device at block 205. This preferably uses the real-time updated status information from database 146 (see FIG. 2) at decision block 207. If the security status indicates that the source device complies with the predetermined security policy, the proxy allows the connection at block 209. If not, the proxy refuses the connection at block 211 and redirects the connection to an explanation message (such as a locally generated web page or other message source) at block 213. In either case, method 200 ends at end point 219.

[0047] In possible embodiments, the determination and decision at block 207 apply a comprehensive minimum policy set that protects other devices in subnet 130 (see FIG. 1) from viruses, trojans, worms, and other malware that might be inadvertently and/or carelessly acquired due to the requested connection.

[0048] In another embodiment, a security information management system is provided, wherein client-side devices preferably collect and monitor information describing the operating system, software, and patches installed on the device(s), as well as configuration thereof. A database of this information is maintained, along with data describing vulnerabilities of available software and associated remediation techniques available for it. The system exposes an API to support security-related decisions by other applications. For example, an intrusion detection system (IDS) accesses the database to determine whether an actual threat exists and should be (or has been) blocked.

ForcePoint LLC
EX-1002
Page023

[0049] In another form of this embodiment, client software runs on each monitored device and reports configuration information to the database, so that the database has substantially real-time-current information.

[0050] The present embodiment of the present invention advantageously acquires the real-time status information from each client using client-side software. In this manner, a resource burden of monitoring is spread among the devices being monitored, and uses far fewer network resources in the process.

[0051] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as the Windows Registry on Microsoft Windows operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0052] In one embodiment, a system maintains a database of vulnerabilities and associated remediation techniques. The remediation techniques include software patches, policy settings or changes, and registry settings or changes. This multi-faceted provides novel flexibility in management of security issues, and convenience for security administrators in both determining available options and selecting remediation steps for vulnerable systems.

[0053] In another embodiment of the present invention, patches, policy changes, software updates, and configuration changes are rolled out to devices on a network using a staged roll-out technique. In this technique, the change is applied to a selected device or set of devices identified by an administrator. After a predetermined amount of time passes, unless the administrator has canceled the roll-out, the change is applied to an additional group of devices on the network. Third- and fourth-tier groups may also be identified by the administrator, where implementation of the remediation or upgrade is automatically effected in subsequent stages a predetermined amount of time after the preceding stage roll-out. Thus, if no failures are noted following a more limited roll-out (on a first set of devices), then the remediation or upgrade is automatically applied to other devices. If, on the other hand, an error or failure is observed, the subsequent roll-out can be canceled so that further failures and problems are avoided.

ForcePoint LLC
EX-1002
Page024

[0054] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0055] In one possible embodiment, provided is a platform and underlying back end that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0056] The latest network compromises are combining qualities of viruses, worms, and denial of service attacks into new blended attacks. Additionally, blended attacks may now utilize metamorphic or polymorphic abilities to change their signatures to avoid detection. To mitigate these new risks, organizations are now deploying a multi-tiered network defense strategy comprised of a variety of network security components layered at the perimeter and to internal network machines and devices. The security components are managed separately, and possibly their data is ported into a Security Information Management System (SIMS) correlation engine.

[0057] However, network security components and correlation engines rely on signatures or anomalies, producing an ever-increasing quantity of data, including false positive, benign, and erroneous events. They also lack the intelligence to identify, reference, or remediate the vulnerabilities targeted by the attack. Furthermore, the time and cost to acquire, manage, and maintain these numerous network security components is overwhelming the end user. Therefore, more sophisticated technology is provided to resolve these performance and management issues.

[0058] In one embodiment, technology may be provided that addresses these requirements by making each security component smarter and provides managers with remote remediation options. Thereby, improving system performance and streamlining management processes.

[0059] In one embodiment, an intelligent integration platform and SDK are provided to meet the above requirements.

ForcePoint LLC
EX-1002
Page025

[0060] In one embodiment, security products are enhanced and system intelligence may be provided. The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats.

[0061] One embodiment cross-references the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable.

[0062] In one embodiment, network vulnerabilities are identified. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0063] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0064] Examples of Anti-Vulnerability applications that may be integrated into network security products for enterprise and small office home office (SOHO) networks when integrated with one embodiment, via the SDK, will be described.

[0065] In one embodiment, update or patch deployment are provided, which remotely remediate network vulnerabilities and provide policy compliance and enforcement capabilities. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix upgrades.

[0066] In one embodiment, an IDS may be provided that accurately determines if the targeted machine is actually vulnerable to an attack; virtually eliminates false positives and false negatives; and adds vulnerability remediation and policy compliance and enforcement functionalities.

[0067] In one embodiment, a scanner may be provided that virtually eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities.

ForcePoint LLC
EX-1002
Page026

[0068] In one embodiment, a firewall may be provided that virtually eliminates false positive and false negatives, preventing the security system from denying valid traffic to the organization – self-inflicted denial of service attacks - and adds vulnerability remediation, and policy compliance and enforcement functionalities.

[0069] In one embodiment, vulnerability management may be provided, as set forth above.

[0070] In one embodiment, multiple products are provided including an IDS, scanner, and firewall. Each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats.

[0071] In one embodiment, change management may be provided, which may automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

[0072] Lastly, the platform may also provide product upgrades and signature updates to each of these various security products.

[0073] The platform is comprised of the following software components: SDK, client agent, logic engine, and data warehouse stored on a dedicated on-site server. Network operations center (NOC) Servers periodically synchronize the customers' servers with the latest vulnerability and update data. See FIG. 5B.

[0074] The same client agent and on-site server support all security applications that are integrated onto the platform, thereby providing the added anti-vulnerability functionalities presented in the previous section.

[0075] There are two system requirements: TCP/IP connectivity, and supported network machines and devices. In one embodiment, platforms supported are set forth below in Table 1.

Table 1

ForcePoint LLC
EX-1002
Page027

All Windows Operating Systems and their applications
All UNIX variants
Cisco routers and firewalls
Toshiba network devices
Netgear network devices
Linksys network devices, including wireless access points

[0076] Platform support is scalable to any network size or architecture; consumer, small office home office (SOHO), enterprise, and distributed networks.

[0077] In one embodiment, technology may be provided that includes a backend platform that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application, update application and the intelligent IDS. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0078] As shown in FIG. 5B, the technology may meet market requirements, presented in the next section.

[0079] For example, networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with compromise attacks. To protect the network, administrators have traditionally set up perimeter defense strategies.

[0080] These strategies generally call for network managers to lock down core servers, and monitor/scan/filter all incoming and outgoing traffic at the network perimeter with several network security products such as antivirus and firewalls to identify and attempt to neutralize hackers and malicious code. In the past, these strategies worked well, however new threats are becoming more complex.

[0081] The latest malicious code may combine qualities of viruses, worms, and direct compromise attacks into new blended attacks. Virus payloads are becoming more complex and

ForcePoint LLC
EX-1002
Page028

by using metamorphic or polymorphic abilities, viruses are able to change their signatures to avoid the fingerprint-type filtering that most applications employ.

[0082] To mitigate these new risks, organizations deploy a multi-tiered network defense strategy comprised of a variety of additional network security products layered at the perimeter and to internal network machines and devices. Such network security products include antivirus, firewall, scanners, and network and host based intrusion detection systems.

[0083] Each of these systems is based on specific signatures, rules, or anomalies of each attack and their variants, and do not identify and remediate the specific network vulnerabilities the attack is targeting. So each attack, and its variants, must be identified and analyzed, a signature prepared, then finally deployed to each point product on each customer's network. This process is uncoordinated among multiple disparate systems, and creates an ever-increasing number of signatures producing more and more attack alerts requiring immediate attention – many of which are erroneous. The security components are managed separately, and possibly their data is ported into a security information management system (SIMS) correlation engine.

[0084] Additionally, to proactively remediate the vulnerabilities the malicious code is targeting, administrators quickly and diligently update or "patch" each network machine and device, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives may require higher standards of network security and integrity to protect consumer privacy, and they are documented with change tracking and audit trail reports.

[0085] Therefore, it is increasingly difficult and costly to effectively mitigate new threats and manage numerous systems — particularly in an environment of rising security standards and policy compliance requirements.

[0086] Thus, the multi-tiered network defense strategy is falling short primarily for four reasons. First, there is an inability of multi-tiered network security products to communicate and share information necessary to mitigate blended threats, and minimize false positives and false negatives. The vulnerabilities targeted by malicious code are not accurately identified nor proactively remediated. The associated excessive aggregate cost of ownership of multiple systems. The excessive administrative burden and cost of managing and maintaining multiple systems.

ForcePoint LLC
EX-1002
Page029

[0087] Hence, there is a need to integrate systems, share information intelligently to better defend against blended threats, reduce management and cost requirements, and automate vulnerability identification and remediation functionalities, as presented in the high-level requirements.

[0088] In one embodiment, technology is provided to meet the following market requirements: integrate network security products to share information; provide system intelligence; and remediate network vulnerabilities.

[0089] In one embodiment, technology may integrate with and enable network security products to intelligently reference and share information from the same vulnerability data set, provide vulnerability identification and remediation functionalities, and efficiently meet policy compliance and enforcement requirements.

[0090] In one embodiment, the platform is a complimentary network security technology. When integrated into the defense strategy, it adds intelligence that more accurately and efficiently mitigates blended threats and offloads the time-consuming functions that burden network administrators.

[0091] In one embodiment, the platform enables network security products to share information via its proprietary logic engine to automatically cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat. Previously separate and uncoordinated processes are now more intelligent and automated, resulting in improved system accuracy and efficiency. Therefore the need to layer more and more point products and add a SIMS is reduced, in-turn decreasing the amount of data – particularly erroneous data – to manage. Subsequently, the costs to acquire, operate, and manage the additional multiple point products, and the need to implement a SIMS, are also reduced.

[0092] In one embodiment, the platform may also remotely and proactively remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented.

ForcePoint LLC
EX-1002
Page030

[0093] In one embodiment, the present technology fulfills market requirements noted in the previous section. For example, it may integrate network security products and provides system intelligence. The same vulnerability data warehouse information is shared with all products so that more intelligent actions may then be taken to mitigate complex threats.

[0094] Still yet, it may cross-reference the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable. Thereby, minimizes erroneous, benign, and false positive data produced by each security product.

[0095] One embodiment identifies network vulnerabilities. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0096] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0097] Various possible benefits include blended attacks being more effectively mitigated and the overwhelming management and maintenance burden on administrators to purchase, operate, and maintain multiple network security products being reduced, while increasing productivity, reducing costs, and more effectively and efficiently meeting policy compliance and enforcement requirements.

[0098] Table 2 illustrates a plurality of end user details.

Table 2

- Supplements existing technology to better defend against blended attacks

ForcePoint LLC
EX-1002
Page031

- Intelligently accesses the vulnerability data warehouse, and remediates vulnerabilities.
- Offers policy compliance and enforcement functionality
- Vulnerabilities may be automatically remediated, verified and documented, therefore enforcing compliance.
- No additional software or hardware implementation costs
- Anti-Vulnerability functionalities may be integrated into existing product platforms.
- Reduces cost of ownership of multi network security products
- Shared vulnerability data sets and added vulnerability remediation functionalities may reduce the number of network security products needed to adequately attain defense strategy requirements.
- Reduces management and maintenance costs
- Increased accuracy of vulnerability identification, remediation and policy enforcement, and reduction of false positives, false negatives and denial of service (DoS), significantly reduces management time and costs.
- Manage more machines and devices on the network through one portal
- Vulnerability remediation and policy compliance and enforcement may be integrated with existing security network security products, and their respective interfaces.
- Minimize end user education/ absorption costs
- Anti-Vulnerability applications are transparently integrated, retaining pre-existing architecture, processes, and interfaces. Therefore, the end user experience remains the same, or improved with simplified or automated processes.
- User experience remains the same – additional time or costs to understand and execute new technologies are minimized
- Anti-Vulnerability applications may be integrated transparently and seamlessly, and the pre-existing operational processes and user interfaces are virtually unchanged.

ForcePoint LLC
EX-1002
Page032

- Supports both the enterprise and SOHO networks
- Data warehouse contains vulnerabilities and updates for many machines and devices that operate on both enterprise and SOHO networks.
- Applications presented hereinafter

[0099] Examples of applications that may be made available for enterprise and small office home office (SOHO) networks when integrated with Anti-Vulnerability technology via the SDK will now be set forth.

[00100] In one embodiment, update or patch deployment is provided. In one embodiment, a patch management and vulnerability remediation solution is provided. The technology enables products to add accurate vulnerability identification, remediation, verification, and policy compliance functions. With such technology, products may gain intelligence, accuracy and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix updates for widely distributed programs, which may optimize system performance and enhance the consumer experience.

[00101] In one embodiment, an IDS is provided. IDS products attempt to identify malicious code by signatures at both the network and host client level. While they may be able to identify malicious code by CVE ID or other identifier, and targeted machines by IP address, but they generally do not have the intelligence to determine if the any of the machines on the network are susceptible to that attack, or with finer granularity, if any machine has a specific vulnerability to that specific attack, or if the targeted vulnerability has already been patched. For example, if the malicious code has been written as a Windows based attack targeting a Windows vulnerability, is the Destination IP actually running Windows, or a UNIX variant? And, if Windows, is it vulnerable to the attack, or has it already been patched? IDS do not have the intelligence to answer these questions, and incident alerts are generated indiscriminately. Lastly, even if the targeted machine is vulnerable - it remains unremediated – an IDS does not have the capability to remediate it.

ForcePoint LLC
EX-1002
Page033

[00102] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the IDS to access the Anti-Vulnerability logic engine and platform. It may then have the intelligence to determine if any machine on the network is susceptible to the attack, remediate the vulnerability, mitigate the attack, and verify policy compliance. Now, if no machines were susceptible to the attack, it is identified as an event but not an incident, no further data or alert is generated, and a management response is not required. Integrated products may gain intelligence, accuracy, and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks.

[00103] In one embodiment, scanners may be provided. Vulnerability scanners assess each machine on the network for vulnerabilities, and create lists of potential vulnerabilities to the system managers. The lists commonly contain many false positives and false negatives, burdening the system and managers with inaccuracies.

[00104] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the scanner to access the logic engine and platform, and then have the intelligence to determine if the machine has actual vulnerabilities, remediate them, and verify policy compliance. Integrated products may gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money.

[00105] In one embodiment, a firewall may be provided. "Smart" firewalls are based in part on signatures and other similar functionalities as the IDS products described above.

[00106] With the present embodiment, the firewall can determine whether an attack is valid or a false positive, thereby preventing the security system from denying valid traffic to the organization – self-inflicted DoS attacks. Such functionalities and benefits may be available for both the enterprise and SOHO networks.

[00107] In one embodiment, vulnerability management may be provided. Vulnerability management products enable managers to set policy and identify potential network vulnerabilities. They typically do not accurately identify each vulnerability on each network machine and device, nor remediate each vulnerability, meeting policy compliance enforcement requirements.

ForcePoint LLC
EX-1002
Page034

[00108] The present embodiment offers similar functionalities and benefits as the patch deployment products described above. In short, it enables products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement. Such functionalities and benefits are available for both the enterprise and SOHO networks.

[00109] To this end, multiple products may be provided: IDS, scanner, firewall, and vulnerability management. Each product functions as the individual products noted above. Each may be deployed and operated on the network in a multi-tiered network defense strategy. They may be disparate system, and their signatures and update deployment schedules may vary. Therefore, the probability of mitigating a new and complex threat decreases, while management requirements and cost increases.

[00110] In one embodiment, they each may communicate with the same backend data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats. It may also enable the products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement functionalities.

[00111] In one embodiment, change management (CM) may be provided. Existing CM applications control the documentation and logging of change throughout the enterprise. These applications ensure that an organization maintains consistent records of what happened and when. Currently administrators must independently recognize that a security patch/update must be deployed to a computer or group of computers.

[00112] The user enters the request in the system, through the pipelined process of change management the request would be approved, the patch/update would be manually installed by a user, then documented in the change management software that the process has been completed. While CM software assists in documentation, very little if any assistance may be provided to identify the patches/updates needed, nor verifying correct function after the update/patch is installed.

[00113] With the current possible embodiment, change management integration may greatly streamline this process further reducing total cost of ownership, ease of use, and a higher standard of documentation. The products may then automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by

ForcePoint LLC
EX-1002
Page035

vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

[00114] Lastly, one possible embodiment may also provide product upgrades and signature updates to each of these various security products - including all of the technology benefits such as ensuring compliance of signature versions, logging, reporting, and verification of installation.

[00115] Thus, one possible embodiment includes an intelligent platform that may supplement any existing defense strategy. Once integrated with the technology, security products may share the same vulnerability data set to improve automation and accuracy – increasing efficiencies and minimizing false positives and false negatives. It also enables remote identification, management, and remediation of network vulnerabilities, and provides update deployment, validation, and reporting capabilities. Thereby, the technology improves network security and integrity, mitigation of blended threats, while increasing productivity, reducing total cost ownership, and more effectively and efficiently attaining policy compliance and enforcement requirements.

[00116] One embodiment provides IDS intelligence, accuracy and remote patching functions - IDS data output integrated with the aforementioned platform via the SDK. The platform's underlying backend including a logic engine and vulnerability data warehouse provides the added functions and performance.

[00117] Conventional IDS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IDS is overwhelming the end user.

[00118] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues. In one embodiment, an intelligent IDS is provided to meet market requirements. The alert data output from a distribution of Snort is integrated with the platform via the SDK, which may add the following functions.

ForcePoint LLC
EX-1002
Page036

[00119] In one embodiment, it cross-references the threat's identifier with the target's configuration. The CVE ID, or other identifier, and the Destination IP address are fed into the logic engine where it cross-references the threat with the machine's configuration profile.

[00120] In one embodiment, it virtually eliminates false positives and false negatives. The backend accurately determines in real time if the targeted machine is susceptible to the attack. And, if the machine is not susceptible, it is filtered and reported back as an event and not an incident. No further data or alert is generated, and a management response is not required.

[00121] In one embodiment, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function may be provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and document it with change tracking and audit trail reports.

[00122] Table 3 sets forth a plurality of features.

Table 3

Supports Windows and UNIX variants
Determines if targeted machine is vulnerable to an attack in real time
Filters out erroneous, benign and false positive alerts
Remotely patches targeted vulnerabilities in one click
Installs in minutes

[00123] To this end, erroneous, benign, and false positive data is filtered out, and incidents may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00124] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment. As shown in 701, the on-site server periodically initiates communication with the NOC servers. In 702, updates are pulled from the NOC servers to the on-site server. In 703a, a sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-

ForcePoint LLC
EX-1002
Page037

references the data with the backend. In 703b, centralized IDS console filters alerts; separating events from incidents. It also offers administrators remote patching function. In 704, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 705, the logic engine automatically determines which updates are needed to remediate the targeted machine. As shown in 706, appropriate updates are remotely deployed, installed, and validated on each client.

[00125] In one embodiment, the intelligent patch management and vulnerability remediation application automatically updates computer OS and application vulnerabilities before they can be exploited by hackers and viruses.

[00126] Networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with directed compromise attacks. To protect the network, administrators must diligently update or "patch" server and workstation vulnerabilities, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives now require higher standards of network security to protect consumer privacy and proprietary data, which must be documented with change tracking and audit trail reports. Therefore, fully automated technology is provided to resolve these issues.

[00127] In one embodiment, a intelligent application called SysUpdate — the first technology to fully automate the updating and reporting processes, as described below.

[00128] In terms of function, one possible embodiment automatically researches updates. In collaboration with software development companies, it receives updates and their respective compatibility and installation guidelines, which are thoroughly reviewed and tested in a lab for system compatibility and stability. One embodiment automatically and securely downloads, and archives, all updates. Once the updates and guidelines are thoroughly reviewed and tested, they are automatically downloaded to each customer's on-site server, verified with MD5 hashes, and archived in a self-populating patch repository database.

[00129] One possible embodiment automatically determines the update and dependency requirements for all computers on a network, based on their individual operating systems, applications, and previously installed updates. The logic engine automatically matches the tested updates and their guidelines across each computer's configuration profile.

ForcePoint LLC
EX-1002
Page038

[00130] One possible embodiment remotely, securely, and automatically deploys updates to each computer and device. Updates may be tested on a test group, and then queued for release to each computer on the network, consistently in accordance with the policy determined by the network administrator.

[00131] One possible embodiment automatically verifies the updates are installed and running correctly. Each computer's client agent installs the updates, and verifies the files and hashes.

[00132] One possible embodiment automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the management console reporting modules. Additionally, application license audit reports may be generated, which lists software installed on each machine, by license key.

[00133] Table 4 illustrates possible features in one embodiment.

Table 4

Supports Windows, UNIX variants, and network devices
Supports non-Microsoft applications
Logic engine provides system intelligence
Files verified with SHA1 or MD5 hashes
MMC snap-in console with Crystal Reports
AES encryption

[00134] FIG. 8 illustrates an update system, in accordance with one embodiment.

As shown in 801, the on-site server periodically initiates communication with the off-site NOC servers. In 802, updates are pulled from the NOC servers to the on-site server. In 803, the centralized MMC snap-in console offers flexible security policy options and comprehensive reporting capabilities. In 804. agents accurately identifies OS, apps, and updates installed on each client by file versions and hashes. In 805, logic engine automatically determines which updates are needed on each client, taking into account OS, app, and update dependencies. In 806, appropriate updates are automatically deployed, installed, and validated on each client.

ForcePoint LLC
EX-1002
Page039

[00135] In one embodiment, a secure computer log management application is provided with fully automated archiving, querying, and reporting options.

[00136] Best practice directives and government compliancy regulations now require administrators to archive log events over an extended period of time, and extensively document log and audit trail reports. With existing tools, these are time-consuming processes. Furthermore, existing tools transfer logs in clear text and are subject to malicious manipulation, and logs may be lost since few utilize guaranteed delivery protocols. Therefore, the integrity and security of the log data is not assured. In the event of an internal or external compromise, logs may be deleted, manipulated, or the network flooded with decoy log data.

[00137] The present possible embodiment automatically and continuously transfers logs from each computer into a self-configuring, self-populating, maintenance-free database where they may be archived for years on end. The transfer process utilizes AES encryption for authentication between the client and server, and a guarantee delivery protocol — ensuring no data is compromised or lost. Flexible cross-correlation queries may be run from a single, remote viewer console, and the data is then automatically formatted into reports.

[00138] In one embodiment, cross-correlation query type descriptions are provided. Such embodiment may provide the following three flexible cross-correlation queries in Table 5, which provide increasing detail and breadth of filtering/sorting capabilities, respectively.

Table 5

General Queries – This is the default query. It filters or sorts the logs of any one computer, by any one of the three log types.

Specific Queries – Detailed queries across all machines, and all log types.

Advanced Queries – Query across any combination of machines, by any combination of sources, events, and log types, over any period of time.

[00139] In one embodiment, features shown in Table 6 may be provided.

ForcePoint LLC
EX-1002
Page040

Table 6

- Continuously pulls all logs into a central database, which may be archived for years on end
- AES encryption and a guarantee delivery protocol ensure logs are not compromised or lost
- Queries may be across any computer, for any log type, over any time frame
- Automatically generates event log reports — ideal for documenting audit and compliance requirements
- Easy download installation

[00140] In one embodiment, automated reports may be provided. Query data is automatically formatted into professional reports Also, a separate reporting interface is available to generate general, machine, and user statistics. The present embodiment quickly and easily fulfills best practice and government compliance requirements for log event archiving and reporting.

[00141] FIG. 9 shows a configured network, in accordance with one embodiment.

[00142] As shown in 901, the server component automatically configures the application, and the database and communicates with the client agents. In 902, client agents are deployed, which then identifies, manages, and continuously transfers all logs to the server. In 903, all client log data may be automatically archived the self-populating database, for years on end. In 904, from the centralized viewer, general, specific, or advanced cross-correlation queries may be run. See Table 7. Query and statistics data is automatically formatted into professional reports to easily document audit and compliance requirements.

Table 7

ForcePoint LLC
EX-1002
Page041

Filter/Sort By:	**General**	**Specific**	**Advanced**
# of Computers	Any One	Any One	Any
# of Log Types	Any One	All	Any
Period of Time	Last or All	Last or All	Any
# of Event Detail Fields *	By ID Only	Any One	Any

* Defined as Time/Date Written, UserID, ComputerID, EventID, Source, Type, and Category

[00143] One possible embodiment provides best practice security policy templates to proactively and remotely manage and enforce enterprise security compliance policies.

[00144] Best practice and government compliance directives require higher standards of network security to protect consumer privacy and proprietary data, which must be consistently enforced, and documented with change tracking and audit trail reports for compliance verification. Therefore, a fully automated technology is provided to resolve these issues.

[00145] One embodiment offers an intelligent application to manage and enforce security policies — the first technology to fully automate the policy configuration, enforcement, and reporting processes, as described below.

[00146] In one embodiment, centralized, remote management is provided. The policy compliance and enforcement module is managed via the centralized management console - in MMC format, and automates the deployment, assessment, and enforcement of the policy chosen.

[00147] One embodiment provides standardized policies selected from many standardized policy templates recommended by NSA, SANS, US Navy, and ISO 17799, or custom policy options to formulate policies that meet the individual needs of any organization.

[00148] One possible embodiment automatically determines out-of-compliance parameters for all computers and devices on a network. Based on each client's individual policy parameter settings and configuration profile, the system's logic engine automatically reports back each client's out-of-compliance parameters.

ForcePoint LLC
EX-1002
Page042

[00149] In one embodiment, it remotely, securely, and automatically enforces policy to each computer or device. Policy changes may be automatically enforced to each computer or device individually, or by group, consistently in accordance with the policy selected by the network administrator. Policy configuration profiles are transmitted between client agent and server in an AES encrypted format for security and privacy. Policy options may be rolled back with one-click.

[00150] Automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the Management Console's Reporting Center. Table 8 sets forth some possible features.

Table 8

Supports Windows, UNIX variants, and network devices
Supports NSA, SANS, Navy, ISO 17799 and other standardized policies
Logic engine provides system intelligence
One-click policy rollback
Automatically generates change tracking and audit trail reports

[00151] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[00152] As shown in 1001, the on-site server periodically initiates communication with the off-site NOC servers. In 1002, templates, rules, and updates are pulled from the NOC servers to the on-site server. In 1003, a centralized management console offers flexible security policy templates, options, and comprehensive reporting capabilities. In 1004, agents are automatically deployed to each client, accurately identifying which policy parameters, OS, apps, and updates are applied or installed. In 1005, a logic engine automatically determines which clients are out of compliance. In 1006, appropriate policy changes are automatically enforced on each client.

[00153] In one embodiment an intelligent IPS may be provided that provides intelligence, accuracy, real-time prevention, and remote patching functions. In one embodiment, it accurately

ForcePoint LLC
EX-1002
Page043

identifies and prevents malicious code from reaching their destination at the in-line IPS Sensor. Thereafter, a security officer may remotely patch the targeted vulnerability.

[00154] Conventional IDS/IPS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IPS is overwhelming the end user.

[00155] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues, by offering an intelligent IPS to meet market requirements. The alert data output from a standard distribution of Snort is integrated with the platform via the SDK which accurately identifies attacks, and the attack is terminated at the in-line sensor – as described in the following functions.

[00156] One embodiment cross-references the threat's identifier with the target's configuration. The in-line Sensor monitors and processes traffic and sends alert data to the on-site server where its logic engine queries the backend in real-time to determine if the destination IP is vulnerable to the attack.

[00157] One possible embodiment provides enhanced flex response. If the destination IP is vulnerable to the attack, the in-line Sensor is commanded to immediately drop the exploit packets – preventing the attack. Further, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function is also provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and documents it with change tracking and audit trail reports.

[00158] In one embodiment, attacks are accurately identified and mitigated before they reach their targets, and targeted vulnerabilities may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00159] Table 9 illustrates some possible features.

Table 9

ForcePoint LLC
EX-1002
Page044

Supports Windows and UNIX variants
Determines in real-time if targeted machine is vulnerable to an attack, virtually eliminating false positives
in-line Sensor flex response terminates the attack
Remotely patches targeted vulnerabilities in one click
Installs in minutes

[00160] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[00161] As shown in 1101, the on-site server periodically initiates communication with the NOC servers. In 1102, updates are pulled from the NOC servers to the on-site server.

[00162] In 1103a, an IPS in-line sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-references the data with the backend. In 1103b, if the destination IP is vulnerable to the attack, the in-line Sensor is commanded in real-time to drop the malicious packets. As shown in 1104, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 1105, the logic engine automatically determines which updates are needed to remediate the targeted machine, and may be remotely deployed from the IPS console. In 1106, appropriate updates are remotely deployed, installed, and validated on each client.

[00163] In one embodiment, an anti-vulnerability SDK is provided. The SDK was designed to be a simple integration pathway to the Anti-Vulnerability platform backend. The SDK is documented and deliverable. The SDK is compatible with many different programming languages such as C, C++, VB, Java, and others.

[00164] The technology is sophisticated, yet all of the details of managing the communications are implemented in the library, requiring the developer to only learn a simple function calls as detailed hereinafter. A product architect chooses the functionality desired, inserts the provided functionality SDK code into the product code. The SDK code may then query – via the logic engine – the data warehouse, and in turn may return an answer to the point product. The architect can then show the results in any format desired in the product's interface.

ForcePoint LLC
EX-1002
Page045

Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well.

[00165] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

[00166] Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience.

[00167] Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy – increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance and enforcement functionalities.

[00168] Anti-Vulnerability functions that are accessible via the SDK. The functions are presented in groups, as follows in Table 10.

Table 10

Session Management
Group Management Functions
Client Management Functions
Patch Management Functions
Polling Functions
User Management Functions
Miscellaneous Functions
Policy Compliance Functions
Session Management Functions

[00169] Table 11 sets forth Session Management Functions

ForcePoint LLC
EX-1002
Page046

Table 11

OpenSession – Parameters: HOST name or IP address, LOGIN and PASSWORD for host
Returns: new SESSION Description: This function opens a new session to the OnSite Server
CloseSession – Parameters: SESSION to close
Returns: None Description: Closes a session that is no longer needed
IsSessionGood – Parameters: SESSION to test
Returns: TRUE or FALSE Description: returns TRUE if the session is still valid FALSE if it is not
SUGetLastError – Parameters: None
Returns: Error code of last error in the thread Description: Returns the error code of the last SDK error to occur in this thread
SUSetLastError – Parameters: ERROR code to set
Returns: None Description: Sets the error code for the thread to be returned by SUGetLastError
GetSDKVersion – Parameters: None
Returns: a WORD containing the version of the SDK Description: the MSB of the returned value is the major version number, the LSB is the minor version number
Ping – Parameters: SESSION to use, VALUE to ping with
Returns: VALUE on success 0 on failure Description: attempts to pass VALUE to the OnSite Server, which should pass it back.

[00170] Table 12 sets forth Group Management Functions.

Table 12

ForcePoint LLC
EX-1002
Page047

CreateGroup – Parameters: Group NAME and Description
Returns: GROUP that was just created or 0 on failure Description: This function creates a new group with the provided name and Description
GetGroups – Parameters: None
Returns: A LIST of GROUPs. Description: This function Returns a list of all configured groups.
GetGroupsEx – Parameters: None
Returns: A LIST of GROUPINFO structures Description: This function Returns a list of all configured groups' information
DeleteGroup – Parameters: GROUP to be deleted.
Returns: Success or failure Description: This function permanently removes a group.
EditGroup – Parameters: GROUP to be edited, GROUPINFO to be applied
Returns: Success or failure Description: This function changes a GROUP's information
GetGroupPolicyOSCategories – Parameters: GROUP to get information about
Returns: A LIST of OPERATINGSYSYTEMCATEGORYs that have group policies configured Description: This function retrieves a list of operating system categories that have group policies configured
GetGroupPolicyOSSubCategories – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get sub category information about
Returns: A LIST of OPERATINGSYSTEMSUBCATEGORYs Description: This function retrieves a list of operating system sub-categories of OPERATINGSYSTEMCATEGORY that have policies for the GROUP
GetGroupPolicyInfo – Parameters: GROUPPOLICY to get information about, GROUPPOLICYINFO pointer to receive the information
Returns: Success or Failure Description: This function fills the passed GROUPPOLICYINFO structure with the information for the GROUPPOLICY

ForcePoint LLC
EX-1002
Page048

GetGroupPolicyInfoByOSCat – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get the policy for, GROUPPOLICYINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMCATEGORY in the GROUP
GetGroupPolicyInfoByOSSubCat – Parameters: GROUP to get information about, OPERATINGSYSTEMSUBCATEGORY to get the policy for, GROUPPOLICYINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMSUBCATEGORY in the GROUP
DeleteGroupPolicy – Parameters: GROUPPOLICY to delete
Returns: Success or failure Description: This function permanently deletes the GROUPPOLICY
EditGroupPolicy – Parameters: GROUPPOLICYINFO with new information
Returns: Success or failure Description: This function updates the group policy (contained in GROUPPOLICYINFO) with the information in GROUPPOLICYINFO
AddGroupPolicy – Parameters: GROUP to add the policy to, GROUPPOLICYINFO containg the policy information
Returns: Success or Failure Description: This function creates a new group policy and applies it to the GROUP
GetClientsInGroup – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTs belonging to the group Description: This function retrieves a list of clients that are members of a specific group
GetClientsInGroupEx – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTINFOs for clients belonging to the group Description: This function Returns a list of CLIENTINFO structures containing

ForcePoint LLC
EX-1002
Page049

information for the clients that belong to this group
AddClientToGroup – Parameters: CLIENT to add to a group, GROUP to add the client to.
Returns: Success or failure Description: This function adds a client to a group
RemoveClientFromGroup – Parameters: CLIENT to remove from group, GROUP to remove the client from
Returns: Success or failure. Description: This function removes a client from a group.
MoveClientToGroup – Parameters: CLIENT to move, GROUP to move client to
Returns: Success or Failure Description: This function moves CLIENT to GROUP
GetUngroupedClients -- Parameters: None
Returns: LIST of ungrouped clients Description: This function Returns a LIST of the clients that do not belong to any group
GetUngroupedClientsEx – Parameters: None
Returns: LIST of CLIENTINFO structures Description: This function Returns a LIST of CLIENTINFO structures for the clients that do not belong to any group
GetGroupInfo – Parameters: GROUP to get information about, GROUPINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for the GROUP

[00171] Table 13 sets forth Client Management Functions.

Table 13

GetClientInstalledSoftware – Parameters: CLIENT to get information about

ForcePoint LLC
EX-1002
Page050

Returns: LIST of SOFTWARE installed on the client Description: This function retrieves a list of the software that has been detected on the client
GetClientInstalledSoftwareEx – Parameters: CLIENT to get information about
Returns: LIST of SOFTWAREINFO for software installed on the client Description: This function returns a LIST of SOFTWAREINFO structures describing the software detected on the client
GetClientInstalledPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the installed patches on the client Description: This function retrieves a list of patches that were verified as installed on the last polling
GetClientInstalledPatchesEx – Parameters: CLIENT to get information from
Returns: LIST of PATCHINFO structures corresponding to the installed patches on the client Description: This function retrieves a LIST of PATCHINFO structures for patches that were verified as installed on the last polling
GetClientPendingPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the pending patches for the client Description: This function returns a list of patches that the client needs (according to group policy) as of the last polling.
GetClientPendingPatchesEx – Parameters: CLIENT to get information from
Returns: A LIST of PATCHINFO structures corresponding to the pending patches for the client Description: This function returns a LIST of PATCHINFO structures for patches that the client needs (according to group policy) as of the last polling.
GetClientPendingServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK if a service pack is pending or 0 if not Description: This function returns a SERVICEPACK if there is a service pack pending for the client (according to group policy) as of the last polling. If there is no service pack pending it returns 0

ForcePoint LLC
EX-1002
Page051

GetClientPendingSoftware – Parameters: CLIENT to get information from
Returns: LIST of SOFTWARE that is pending Description: This function returns a list of software that is pending for the client (according to group policy) as of the last polling
GetClientLogs - Parameters: CLIENT to get information from
Returns: LIST of LOGs for the client. Description: This function returns a list of logs for a particular client.
GetClientLogsEx – Parameters: CLIENT to get information from
Returns: LIST of LOGINFO structures Description: This function returns a list of LOGINFO structures containing log entries for a particular client.
DeleteClient – Parameters: CLIENT to delete.
Returns: Success or failure. Description: This function removes all information pertaining to this client from the SysUpdate database.
GetClientOS – Parameters: CLIENT to get information from
Returns: OPERATINGSYSTEM installed on client Description: This function returns the OPERATINGSYSTEM installed on the client
GetClientServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK installed on client or 0 Description: This function returns the service pack installed on the client or 0 if the client does not have a service pack installed, or if service packs are not applicable to the client's platform
GetClientInfo – Parameters: CLIENT to get information from CLIENTINFO pointer to receive the information
Returns: Success or failure Description: This function fills the passed CLIENTINFO structure with information pertaining to the passed CLIENT
GetClientFromIP – Parameters: IP address of client
Returns: CLIENT that corresponds to the passed IP address

ForcePoint LLC
EX-1002
Page052

Description: This function maps IP addresses to clients

[00172] Table 14 sets forth Patch Management Functions.

Table 14

GetPatchInfo – Parameters: PATCH to get information about, PATCHINFO pointer to receive information
Returns: Success or failure Description: This function fills the passed patch info structure with information about the passed patch
InstallPatchForClient – Parameters: CLIENT to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to the client. Installation proceeds asynchronously
InstallPatchForGroup – Parameters: GROUP to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to all clients in the group
InstallAllPendingForClient – Parameters: CLIENT to install patches on
Returns: Success or failure Description: This function deploys all pending patches for a client to the client
InstallAllPendingForGroup – Parameters: GROUP to install patches on
Returns: Success or failure Description: This function deploys all pending patches to all clients in a group
RejectPatchForClient – Parameters: CLIENT to reject patch for, PATCH to reject
Returns: Success or failure Description: This function rejects a patch for a client. This patch will not be queued down or installed
RejectPatchForGroup – Parameters: GROUP to reject patch for, PATCH to reject
Returns: Success or failure

ForcePoint LLC
EX-1002
Page053

Description: This function rejects a patch for every client in a group. This patch will not be queued down or installed
RequeuePatchForClient – Parameters: CLIENT to requeue the patch for, PATCH to requeue
Returns: Success or failure Description: This function requeues a previously rejected patch for a client
RequeuePatchForGroup – Parameters: GROUP to requeue the patch for, PATCH to requeue
Returns: Success or failure Description: This function requeues a previously rejected patch for every client in a group
RemovePatchFromClient – Parameters: CLIENT to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch from a client
RemovePatchFromGroup – Parameters: GROUP to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch for every client in a group
InstallServicePackForClient – Parameters: CLIENT to install service pack on, SERVICEPACK to install on client
Returns: Success or failure Description: This function will install a service pack on a client
InstallServicePackForGroup – Parameters: GROUP to install service pack on, SERVICEPACK to install
Returns: Success or failure Description: This function will install a service pack on every client in a group
InstallSoftwareForClient – Parameters: CLIENT to install software update on, SOFTWARE to install
Returns: Success or failure Description: This function will install a software update on a client
InstallSoftwareForGroup – Parameters: GROUP to install software update on, SOFTWARE to install
Returns: Success or failure

ForcePoint LLC
EX-1002
Page054

Description: This function will install a software update on every client in a group.
GetCveIDsFromPatch – Parameters: PATCH to get CveIDs from
Returns: A LIST of CVEIDs Description: This function returns a list of CVEIDs the correspond to the PATCH

[00173] Table 15 sets forth Polling Functions.

Table 15

PollClient – Parameters: CLIENT to poll
Returns: Success or failure. Description: This function causes a client to be polled by the OnSite Server immediately.
PollGroup – Parameters: GROUP to poll
Returns: Success or failure. Description: This function causes all the clients in a particular group to be polled immediately.
PollAll – Parameters: NONE
Returns: Success or failure. Description: This function causes all clients to be polled immediately.

[00174] Table 16 sets forth User Management Functions.

Table 16

GetUsers – Parameters: None
Returns: A LIST of USERs Description: This function returns a list of all users for the system
GetUserInfo – Parameters: USER to get information about, USERINFO pointer to receive the

ForcePoint LLC
EX-1002
Page055

information
Returns: Success or failure Description: This function populates the passed USERINFO structure with information about the passed USER
GetUserGroupPrivileges – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEs Description: This function returns a LIST of USERGROUPPRIVILEGES representing the privileges that a particular user has
GetUserGroupPrivilegesEx – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEINFO structures Description: This function returns a LIST of USERGROUPPRIVILEGEINFO structures representing the privileges that a particular user has
GetUserGroupPrivilegeInfo – Parameters: USERGROUPPRIVILEGE to get information about, USERGROUPPRIVILEGEINFO pointer to receive information
Returns: Success or failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the details of the particular privilege
GetUserGroupPrivilegeInfoByGroup – Parameters: USER to get information about, GROUP to get information for, USERGROUPPRIVILEGEINFO pointer to populate
Returns: Success or Failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the detailed information regarding the permissions that the passed user has on the passed group
AddUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO structure to add
Returns: Success or failure Description: This function adds a USERGROUPPRIVILEGE
EditUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO with new values
Returns: Success or failure Description: This function edits the USERGROUPPRIVILEGEINFO structure passed in, assign it the new values

ForcePoint LLC
EX-1002
Page056

DeleteUserGroupPrivilege – Parameters: USERGROUPPRIVILEGE to delete
Returns: Success or failure Description: This function deletes the passed USERGROUPPRIVILEGE from the system
AddUser – Parameters: USERNAME, PASSWORD, and USERTYPE
Returns: USER representing the user that was just created Description: This function creates a new user with the provided username, password, and type, and returns a USER representing the new user or 0 in the case of an error
DeleteUser – Parameters: USER to delete
Returns: Success or failure Description: This function permanently deletes the USER from the system along with any privileges the user may have had
ChangeUserPassword – Parameters: USER to change password for, new PASSWORD
Returns: Success or failure Description: This function changes the password for a user
ChangeUserRole – Parameters: USER to change role, ROLE to change to
Returns: Success or failure Description: This Function changes a user's role
GetUserFromName – Parameters: USERNAME
Returns: USER corresponding to the passed user name Description: This function provides a mapping from user names to USERs

[00175] Table 17 sets forth Miscellaneous Functions.

Table 17

CreateList – Parameters: None
Returns: A new, empty, LIST Description: This functions creates a new LIST that is initially empty

ForcePoint LLC
EX-1002
Page057

GetListItemEx – Parameters: LIST to retrieve item from, INDEX of item to retrieve, VOID pointer to receive item
Returns: Success or failure Description: This function populates the memory pointed to by VOID with the contents of the LIST item at INDEX
GetListSize – Parameters: LIST to get the size of
Returns: the size of the LIST Description: This function returns the number of elements currently in the list
AddItemToList – pointer to LIST to add the item to, LONG item to add
Returns: None Description: This function adds an "item" (such as a GROUP or a CLIENT) to a LIST
AddClientInfoExToList – See AddItemToList
AddGroupInfoToList – See AddItemToList
AddPatchInfoExToList – See AddItemToList
AddSoftwareInfoToList – See AddItemToList
AddSoftwareCategoryInfoToList – See AddItemToList
AddUserGroupPrivilegeInfoExToList – See AddItemToList
RemoveItemFromList – Parameters: pointer to LIST to remove the item from, INDEX of item to remove
Returns: None Description: This function removes the item at INDEX from the LIST
FreeList – LIST to deallocate
Returns: None Description: This function deallocates the resources used by LIST
GetSoftwareInfo – Parameters: SOFTWARE to get information for, SOFTWAREINFO pointer to hold the information
Returns: Success or failure Description: This function populates the SOFTWAREINFO structure pointed at with information regarding the SOFTWARE
GetLogInfo – Parameters: LOG to get information about, LOGINFO pointer to contain the

ForcePoint LLC
EX-1002
Page058

information
Returns: Success or failure Description: This function populates the LOGINFO structure pointed at with information regarding the LOG
GetSoftwareCategories – Parameters: None
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of SOFTWARECATEGORYs
GetSoftwareCategoriesEx – Parameters: None
Returns: A LIST of SOFTWARECATEGORYINFO structures Description: This function returns LIST of SOFTWARECATEGORYINFO structures for every software category known on the system
GetSoftwareCategoriesForOperatingSystemCategory – Parameters: an OPERATINGSYSTEMCATEGORY to get information for
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of software categories for the passed operating system category.
GetSoftwareCategoriesForOperatingSystemCategoryEx – As above only, returning the appropriate “info” structures in the list
GetSoftwareCategoryInfo – Parameters: SOFTWARECATEGORY to get information for, SOFTWARECATEGORYIFNO pointer to contain the information Returns: Success or failure

[00176] Table 18 sets forth Policy Compliance Functions.

[00177] These functions are provided in a separate source tree (policy tree) for the Policy Compliance and Enforcement module. Function include: Password/system access policies, log configurations, audit settings, user/group privilege rights, general service settings, service permissions, registry values, registry permissions, file permissions. It can also perform deltas on and get information about: groups, users, services, and all the "Run" registry keys.

[00178] The function calls are being integrated into the live production tree and subject to change.

ForcePoint LLC
EX-1002
Page059

Table 18

GetPolicyItemInfo – As GetOperatingSystemInfo for POLICYITEM and POLICYITEMINFO
InstallPolicyItemForClient – As InstallPatchForClient for POLICYITEM
InstallPolicyItemForGroup – As InstallPatchForGroup for POLICYITEM
InstallAllPendingPolicyItemsForClient – As InstallAllPendingPatchesForClient for POLICYITEM
InstallAllPendingPolicyItemsForGroup – As InstallAllPendingPatchesForGroup for POLICYITEM
RemovePolicyItemFromClient – As RemovePatchForClient for POLICYITEM
RemovePolicyItemFromGroup – As RemovePatchFromGroup for POLICYITEM

[00179] All publications, prior applications, and other documents cited herein are hereby incorporated by reference in their entirety as if each had been individually incorporated by reference and fully set forth.

[00180] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only the preferred embodiments have been shown and described and that all changes and modifications that would occur to one skilled in the relevant art are desired to be protected.

ForcePoint LLC
EX-1002
Page060

CLAIMS

What is claimed is:

1. An apparatus, comprising:

at least one data storage;

at least one platform communicatively coupled to the at least one data storage; and

at least one agent capable of being communicatively coupled to the at least one platform;

said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

said at least one platform configured to:

cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability;

ForcePoint LLC
EX-1002
Page061

said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability;

said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

2. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to user input received prior to the attack, the firewall option is capable of being applied to a plurality of different devices for preventing the at least one attack packet at any of the different devices; and the apparatus is further configured such that, in response to additional user input after the attack in connection with a particular single device of the plurality of different devices, the intrusion detection or prevention option is capable of being applied to the particular single device.

3. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to user input prior to the attack, the intrusion detection or prevention option is capable of being applied to a plurality of different devices at the plurality of different devices; and the apparatus is further configured such that, in response to user input after the attack in connection with a particular single device of the plurality of different devices, the firewall option is capable of being applied to the particular single device for preventing the at least one attack packet at the particular single device.

4. The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification

ForcePoint LLC
EX-1002
Page062

of the operating system in connection with the accessing for the displaying of the at least one mitigation technique, so that, in order to avoid false positives, relevant vulnerabilities prompt mitigation technique user selection among at least two of the mitigation techniques, which involve both firewall and intrusion prevention system actions, for providing diverse mitigation options in connection with the relevant vulnerabilities.

5. The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system prior to causing the display of the at least one mitigation technique, so that which of the one or more of the mitigation techniques that is caused to be displayed is based on one or more actual vulnerabilities to which the at least one device is actually vulnerable so that only relevant one or more mitigation techniques are displayed for selection by a user for attack mitigation.

6. The apparatus of Claim 1, wherein the apparatus is configured such that the user input is capable of being received via at least one user interface of the at least one platform for different devices, for allowing different attack mitigation actions including at least one intrusion prevention action and at least one firewall action to be selectively applied to the different devices for different actual vulnerabilities determined to be actually relevant based on the identification of the operating system in connection with the different devices.

7. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a first mitigation technique that utilizes a firewall action and a second mitigation technique that utilizes an intrusion prevention action;

8. The apparatus of Claim 7, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first

ForcePoint LLC
EX-1002
Page063

mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

9. The apparatus of Claim 7, wherein the apparatus is configured such that the at least one mitigation technique further includes a third mitigation technique that utilizes a policy compliance action, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique, the second mitigation technique, and the third mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device; only the second mitigation technique being selectively applied by the user to at least one second device; and the first mitigation technique, the second mitigation technique, and the third mitigation technique being selectively applied by the user to at least one third device.

10. The apparatus of Claim 7, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from an integrated firewall/intrusion prevention system platform component of the at least one platform to firewall-supporting code of the at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the integrated firewall/intrusion prevention system platform component of the at least one platform to intrusion prevention system-supporting code of the at least one agent, where the firewall-supporting code and the system-supporting code are part of the at least one agent.

11. The apparatus of Claim 1, wherein the apparatus is configured such that the identification of the operating system is a result of a vulnerability assessment scan caused by the at least one platform.

ForcePoint LLC
EX-1002
Page064

12. The apparatus of Claim 1, wherein the at least one platform includes intrusion prevention functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality.

13. The apparatus of Claim 1, wherein the at least one platform utilizes router-based functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique.

14. The apparatus of Claim 13, wherein the apparatus is configured such that the system is capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the router-based functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the router-based functionality and the firewall functionality.

15. The apparatus of Claim 1, wherein at least one of:

said at least one data storage includes at least one database;

said at least one data storage is accessed by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said mitigation techniques include remediation techniques;

each mitigation technique has a mitigation type including the patch;

each mitigation technique has a mitigation type including the policy setting;

ForcePoint LLC
EX-1002
Page065

each mitigation technique has a mitigation type including the configuration option;
each mitigation technique is capable of mitigating the effect of the attack that takes advantage of the corresponding vulnerability, by dropping packets associated with the attack or removing the corresponding vulnerability;
said information is capable of being used to determine an intended destination of a connection request; or
said information includes a vulnerability identifier;
wherein the apparatus is operable for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation technique; and wherein the apparatus is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

16. An apparatus, comprising:

at least one data storage configured to store at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; and

at least one platform communicatively coupled to the at least one data storage, the at least one platform configured to:

based on user selection, automatically apply at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation

ForcePoint LLC
EX-1002
Page066

type and at least one second mitigation technique of a second mitigation type to the at least one device;

receive information in connection with at least one of a plurality of devices,

identify an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information, and

mitigate an effect of the attack on the at least one device that takes advantage of the at least one vulnerability, based on the application;

wherein the apparatus is configured such that the at least two of the plurality of mitigation techniques are made available for the user selection, based on an identification of an operating system.

17. The apparatus of Claim 16, wherein the apparatus is configured such that the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by at least one agent that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

18. The apparatus of Claim 17, wherein the apparatus is configured such that the at least one agent is further capable of supporting a vulnerability assessment scan for the identification of the operating system.

19. The apparatus of Claim 16, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from the at least one platform to firewall-supporting code of at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the at least one platform to intrusion prevention system-supporting code of the at least one agent; wherein the at

ForcePoint LLC
EX-1002
Page067

least one platform includes intrusion prevention functionality for supporting the first mitigation technique and firewall functionality for supporting the second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally make available for the user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

20. An apparatus, comprising:

means for identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities associated with an operating system, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

means for:

ForcePoint LLC
EX-1002
Page068

causing display of at least two of the mitigation techniques for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allowing receipt of at least one user input in connection with one or more of the at least two mitigation techniques; and

means for automatically applying the one or more of the at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device;

said apparatus configured such that the at least two mitigation techniques are displayed based on an identification of an operating system.

ForcePoint LLC
EX-1002
Page069

ABSTRACT

A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

ForcePoint LLC
EX-1002
Page070

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	70	70
UTILITY SEARCH FEE	2111	1	300	300
UTILITY EXAMINATION FEE	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**730**

Electronic Acknowledgement Receipt	
EFS ID:	29348550
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	30-MAY-2017
Filing Date:	
Time Stamp:	22:50:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$730
RAM confirmation Number	053117INTEFSW22522100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	SP1P012C_ADS_vF_30-May-2017.pdf	82768 506e85b05f631b905d273385a91ea248617b5196	no	7
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2	Oath or Declaration filed	SP1P012C_Decl-B_vF_30-May-2017.pdf	161834 c8b4499be702a8762842cc2f7be4e04cd2471f13	no	1
Warnings:					
Information:					
3	Oath or Declaration filed	SP1P012C_Decl-O_vF_30-May-2017.pdf	251207 a0aff797f96e944e54cdb3c22205503192be4e0c	no	1
Warnings:					
Information:					
4	Power of Attorney	SP1P012C_POA_vF_30-May-2017.pdf	889866 e19e0ec50fe66be16de9e2d222db74a8be723f19	no	1
Warnings:					
Information:					
5	Drawings-only black and white line drawings	SP1P012C_Figs_vF_30-May-2017.pdf	3168465 103aec936ef7ab58a38fa3667e79b01ff0e9dce6	no	12
Warnings:					
Information:					
6		SP1P012C_App_vF_30-May-2017.pdf	238148 17fa3bb924645cfa93980924 91fb18496601959d	yes	57

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	47
	Claims	48	56
	Abstract	57	57

Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	34944 faed7be541c1e3378cf9d9efc6980740a154214f	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4827232		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Brett	M.	Oliphant	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Plano	State/Province	TX	Country of Residence	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC		
Address 2	318 West Dogwood		
City	Woodville	State/Province	TX
Postal Code	75979	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	P.	Blignaut	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	West Lafayette	State/Province	IN	Country of Residence	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC		
Address 2	318 West Dogwood		
City	Woodville	State/Province	TX
Postal Code	75979	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	92045		
Email Address	pcaldwell@thecaldwellfirm.com	Add Email	Remove Email

Application Information:

Title of the Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION		
Attorney Docket Number	SP1P012C	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	92045		

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14816931	2015-08-03
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14816931	Continuation of	14499230	2014-09-28	9100431	2015-08-04

Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14499230	Continuation in part of	14138014	2013-12-21	9117069	2015-08-25

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14138014	Continuation of	10882852	2004-07-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10882852	Claims benefit of provisional	60484085	2003-07-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	SecurityProfiling, LLC		
Mailing Address Information For Applicant:			
Address 1	318 West Dogwood Street		
Address 2			
City	Woodville	**State/Province**	TX
Country	US	Postal Code	75979
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012C
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature	/Patrick Caldwell/			Date (YYYY-MM-DD)	2017-05-30
First Name	Patrick	Last Name	Caldwell	Registration Number	44580

Additional Signature may be generated within this form by selecting the Add button.

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent C o o p eration Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ForcePoint LLC
EX-1002
Page082

Attorney Docket No.: SP1P0012

COMBINED DECLARATION (37 C.F.R. 1.63) AND ASSIGNMENT FOR UTILITY APPLICATION USING AN APPLICATION DATA SHEET (37 C.F.R. 1.76)

Title of Invention: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

As the below named inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked)
☐ United States application or PCT international application number _____, filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, CFR § 1.56.

Whereas, I the undersigned inventor have invented certain new and useful improvements as set forth in the above-identified patent application and further identified by the Attorney Docket Number provided above in the header of this document.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I the undersigned inventor hereby:

1) Sell(s), assign(s) and transfer(s) to SecurityProfiling, LLC, a Texas limited liability company having a place of business at 1919 S Shiloh Rd. Garland, TX 75042, (hereinafter referred to as ("ASSIGNEE"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application.

2) Authorize and request the Commissioner of Patents to issue any and all Letters Patents resulting from said application or any division(s), continuation(s), substitutes(s) or reissue(s) thereof to the ASSIGNEE.

3) Agree to execute all papers and documents and, entirely at the ASSIGNEE's expense, perform any acts which are reasonably necessary in connection with the prosecution of said application, as well as any derivative and applications thereof, foreign applications based thereon, and/or the enforcement of patents resulting from such applications.

4) Agree that the terms, covenants and conditions of this assignment shall inure to the benefit of the Assignee, its successors, assigns and other legal representative, and shall be binding upon the inventor(s), as well as the inventor's heirs, legal representatives and assigns.

5) Warrant and represent that I have not entered, and will not enter into any assignment, contract, or understanding that conflicts with this assignment.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Signed on the date indicated beside my signature.

Legal Name of Inventor: John P. Blignaut

Signature: _____ Date: 9.24.14

ForcePoint LLC
EX-1002
Page083

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Brett M. Oliphant Date (Optional): _____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

SCORE Placeholder Sheet for IFW Content

Application Number: 15608978 Document Date: 05/30/2017

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/608,978

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20=	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/608,978	05/30/2017	2431	730	SP1P012C	20	3

CONFIRMATION NO. 9647

92045
The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

FILING RECEIPT

OC000000092013680

Date Mailed: 06/14/2017

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Woodville, TX;

Power of Attorney: The patent practitioners associated with Customer Number 92045

Domestic Priority data as claimed by applicant

This application is a CON of 14/816,931 08/03/2015
which is a CON of 14/499,230 09/28/2014 PAT 9100431
which is a CIP of 14/138,014 12/21/2013 PAT 9117069
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

ForcePoint LLC
EX-1002
Page087

If Required, Foreign Filing License Granted: 06/12/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/608,978**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
**** SMALL ENTITY ****
Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1002
Page088

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: June 15, 2018

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

Before substantive prosecution, please enter the following amendments.

ForcePoint LLC
EX-1002
Page090

Amendments to the Claims:

The listing of amended claims follows:

1.-20. (Cancelled)

21. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices

ForcePoint LLC
EX-1002
Page091

for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

22. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is capable of being applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is capable of being applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device.

23. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that at least two options are provided including a firewall-type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is capable of being applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection

ForcePoint LLC
EX-1002
Page092

with a particular single device of the plurality of devices, the firewall-type option is capable of being applied to the particular single device.

24. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith.

25. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said potential vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said accurately identified vulnerability information is generated via a vulnerability scan operation;

said accurately identified vulnerability information identifies at least one accurately identified vulnerability;

said accurately identified vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the accurately identified vulnerabilities;

ForcePoint LLC
EX-1002
Page093

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is capable of being utilized for identifying the at least one operating system or an application;

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that is capable of taking advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

ForcePoint LLC
EX-1002
Page094

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first accurately identified vulnerability and utilizing a second one of the different occurrence mitigation actions for a second accurately identified vulnerability;

said at least one accurately identified vulnerability is the at least one operating system;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one

ForcePoint LLC
EX-1002
Page095

operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is capable of being caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is capable of being caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one accurately identified vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is accurately identified as being vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

ForcePoint LLC
EX-1002
Page096

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

26. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by:

ForcePoint LLC
EX-1002
Page097

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information; and

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

27. (New) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response

ForcePoint LLC
EX-1002
Page098

to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence.

28. (New) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

29. (New) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that different user input is capable of being received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is capable of resulting in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

ForcePoint LLC
EX-1002
Page099

30. (New) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

31. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by:

C

ForcePoint LLC
EX-1002
Page100

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities;

display information that is based on the accurately identified vulnerability information;

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices;

wherein the at least one configuration involves at least one operating system.

32. (New) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence.

33. (New) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence, resulting in: the utilization of

ForcePoint LLC
EX-1002
Page101

only a first occurrence mitigation action of the firewall-based occurrence mitigation type being caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion mitigation system-based occurrence mitigation type being caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being caused at the third device in response to the occurrence.

34. (New) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

35. (New) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that different user input is capable of being received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is capable of resulting in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion mitigation system-based occurrence mitigation type being

C

ForcePoint LLC
EX-1002
Page102

completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being completed at the third device in response to the occurrence.

36. (New) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

37. (New) The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation.

C

ForcePoint LLC
EX-1002
Page103

Remarks:

The claims have been clarified. It should be noted that no claims are intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-4964 (Order No. SP1P012C).

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

Respectfully submitted,



Dated: 15 Jun 2018

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

C

ForcePoint LLC
EX-1002
Page104

Electronic Acknowledgement Receipt	
EFS ID:	32917141
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	15-JUN-2018
Filing Date:	30-MAY-2017
Time Stamp:	20:40:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	SP1P012C_Prelim_Amend_vF_15-Jun-2018.pdf	99632 3031cb6b58ebc341611cd635904d163b5b8a8bdc	no	15

Warnings:

Information:	
Total Files Size (in bytes):	99632

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 06/22/2018

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TEXAS 75229
UNITED STATES OF AMERICA

EXAMINER	
HERZOG, MADHURI R	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
06/22/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

Office Action Summary	**Application No.** 15/608,978	**Applicant(s)** Oliphant et al.	
	Examiner MADHURI R HERZOG	**Art Unit** 2438	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 06/15/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 21-37 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 21-37 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 05/30/2017 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-20 have been cancelled.

3. Claims 21-37 have been examined and are pending.

Priority

4. Acknowledgement is made of the applicant's claim to priority as a continuation of parent application 14/816931.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*,

ForcePoint LLC
EX-1002
Page109

686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

6. Claim 21-37 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 8984644, claims 1-21 of U.S. Patent No. 9225686, claims 1-154 of U.S. Patent No. 9117069 and claims 1-20 of U.S.

ForcePoint LLC
EX-1002
Page110

Patent No. 9118711. Although the claims at issue are not identical, they are not patentably distinct from each other because:

Claim 21 of the instant application: 21. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities; identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation

ForcePoint LLC
EX-1002
Page111

types across the plurality of devices; wherein the at least one configuration involves at least one operating system.

Is analogous to:

Claim 1 of U.S. Patent No. 8984644: 1. A computer program product embodied on a non-transitory computer readable medium, comprising: code for receiving actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including: at least one first potential vulnerability, and at least one second potential vulnerability; said actual vulnerability information generated utilizing the potential vulnerability information, in response to code execution by at least one processor, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities; code for identifying an occurrence in connection with at least one of the plurality of devices; code for determining that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the actual vulnerability information; and code for providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of

ForcePoint LLC
EX-1002
Page112

devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.

Similarly, the rest of the dependent and independent claims of the instant application are analogous to the rest of the dependent and independent claims of U.S. Patent No. 8984644.

7. Also, claims 21-37 of the instant application are analogous to:

(i) Claims 1-21 of U.S. Patent No. 9225686.

(ii) Claims 1-154 of U.S. Patent No. 9117069.

(iii) Claims 1-20 of U.S. Patent No. 9118711.

8. Claims 21-37 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims 21-47 of copending Application No. 15/608981 (reference application). Although the claims at issue are not identical, they are not patentably distinct from each other because: Claim 1 of the instant application (recited above) is analogous to claim 1 of the 15/608981: 21. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including: at least one first potential vulnerability, and at least one second potential vulnerability; said actual vulnerability information

ForcePoint LLC
EX-1002
Page113

generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities; identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the actual vulnerability information; and permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; wherein the at least one configuration involves at least one operating system.

Similarly, the rest of the dependent and independent claims of the instant application are analogous to the rest of the dependent and independent claims of 15/608981.

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

ForcePoint LLC
EX-1002
Page114

9. Claims 21-37 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims 60-81 of copending Application No. 14/816931 in view of US 7257630 to Cole et al. Claim 21 of the instant application is analogous to claim 60 of 14/816931: An apparatus, comprising: at least one data storage; at least one platform communicatively coupled to the at least one data storage; and at least one agent capable of being communicatively coupled to the at least one platform; said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where: each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; said at least one platform configured to: cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability; said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, so that the at least one mitigation technique is capable of being applied; said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

ForcePoint LLC
EX-1002
Page115

Claim 60 of 14/816931 does not teach the limitations: receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities; and wherein the at least one configuration involves at least one operating system. However, Cole teaches:

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: As described in more detail below, in the vulnerability assessment routine 364, the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine whether the ports of the target computers exhibit the potential vulnerabilities. The method uses information stored in a known vulnerability database 366 to select the vulnerability scripts to executes for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database 344)**;

**ForcePoint LLC
EX-1002
Page116**

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30)**;

wherein the at least one configuration involves at least one operating system **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS)**

ForcePoint LLC
EX-1002
Page117

identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Cole in the invention of 14/816931 to include receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities; and wherein the at least one configuration involves at least one operating system. The motivation to do so would be to provide a comprehensive network vulnerability testing and reporting method and system (Cole: column 2, lines 21-25).

This is a provisional nonstatutory double patenting rejection.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

ForcePoint LLC
EX-1002
Page118

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

11. Claims 21, 26 and 31 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 21 recites the limitations: receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities. The examiner has not found support in the specification of the instant application or the specifications of any of the parent applications for these limitations. More specifically, the examiner has not found support describing the procedure to determine accurately identified vulnerability

ForcePoint LLC
EX-1002
Page119

information of a device based on device configuration and potential vulnerability information.

12. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 22, 23, 25, 29 and 35 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claim 22 recites the limitations: "the firewall-type option is capable of being applied…", "the intrusion prevention-type option is capable of being applied…". The phrase "capable" makes it unclear whether the firewall-type option and the intrusion prevention-type option are actually being applied or not. Similarly, the use of the phrase "capable" in the limitations of claims 23, 25, 29 and 35 also makes the actual implementation of the functions recited in the limitations unclear.

Claim Rejections - 35 USC § 103

14. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

ForcePoint LLC
EX-1002
Page120

matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. This application currently names joint inventors. In considering patentability of the claims under pre-AIA 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of pre-AIA 35 U.S.C. 103(c) and potential pre-AIA 35 U.S.C. 102(e), (f) or (g) prior art under pre-AIA 35 U.S.C. 103(a).

17. Claims 21-37 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7257630 to Cole et al (hereinafter Cole), US 20050193430 to Cohen et al (hereinafter Cohen) and US 20060101517 to Banzhof et al (hereinafter Banzhof).

As per claims 21 and 26, Cole teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

ForcePoint LLC
EX-1002
Page121

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: As described in more detail below, in the vulnerability assessment routine 364, the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine whether the ports of the target computers exhibit the potential vulnerabilities. The method uses information stored in a known vulnerability database 366 to select the vulnerability scripts to executes for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database 344)**;

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as**

determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30);

wherein the at least one configuration involves at least one operating system **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**.

Cole does not teach: identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities

ForcePoint LLC
EX-1002
Page123

utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. However, Cohen teaches:

identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information **(Cohen: [0067]: FIG. 3 is a flow diagram showing a method of verifying actual vulnerabilities in a computer network in accordance with one embodiment of the present invention. To find raw vulnerabilities which could be exploited, the information discovery agents scan the network from the perspective of an attacker by starting attacks, but stopping before too much damage is done. Packets of data are sent to each network device and any responses received back from the network devices are interpreted to determine whether a raw vulnerability exists. The information discovery agent would send packets containing a query command for the BIND server on a network to return its version number. If the BIND server returns a version number which is known to be vulnerable to attacks, the information discovery agent would report the raw vulnerability. [0071]: As such, in some embodiments, the logic can specify pre-conditions for exploitation of vulnerabilities. [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers)**;

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Cohen in the invention of Cole to include identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the accurately identified vulnerability information and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of

ForcePoint LLC
EX-1002
Page125

accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to conduct security assessments automatically in a computer network (Cohen: [0010]).

Cole in view of Cohen teaches intrusion prevention system-based occurrence mitigation type but does not teach a firewall-based occurrence mitigation type. However, Banzhof teaches:

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key**

ForcePoint LLC
EX-1002
Page126

access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole to include allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to provide a computer vulnerability resolution system which utilizes inventory management processes to enhance remediation of vulnerable computer systems forming part of a computer network being remediated by the computer vulnerability resolution system (Banzhof: [0004]).

As per claim 31, Cole teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive accurately identified vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: As described in more detail below, in the vulnerability assessment routine 364, the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine**

ForcePoint LLC
EX-1002
Page127

whether the ports of the target computers exhibit the potential vulnerabilities. The method uses information stored in a known vulnerability database 366 to select the vulnerability scripts to execute for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database 344);

said accurately identified vulnerability information generated utilizing the potential vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities**(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the**

ForcePoint LLC
EX-1002
Page128

ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30);

display information that is based on the accurately identified vulnerability information **(Cole: column 68, lines 58-67: Thus, in one embodiment of the present invention, the reports engine produces (1) a dynamic graphical display representing the network topology, the target computers found, and the vulnerabilities found throughout the target network; (2) a comprehensive list of target computers, vulnerabilities found, and vulnerability explanations)**;

wherein the at least one configuration involves at least one operating system **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**.

Cole does not teach: cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices. However, Cohen teaches:

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion mitigation system-based occurrence mitigation

ForcePoint LLC
EX-1002
Page129

type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Cohen in the invention of Cole to include cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices. The motivation to do so would be to conduct security assessments automatically in a computer network (Cohen: [0010]).

ForcePoint LLC
EX-1002
Page130

Cole in view of Cohen teaches a intrusion mitigation system-based occurrence mitigation type but does not teach a firewall-based occurrence mitigation type. However, Banzhof teaches:

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of

ForcePoint LLC
EX-1002
Page131

Cole to include cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to provide a computer vulnerability resolution system which utilizes inventory management processes to enhance remediation of vulnerable computer systems forming part of a computer network being remediated by the computer vulnerability resolution system (Banzhof: [0004]).

As per claim 22, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is capable of being applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is capable of being applied to the particular single

ForcePoint LLC
EX-1002
Page132

device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Also, Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055])**.

As per claim 23, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that at least two options are provided including a firewall-type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is capable of being applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is capable of being applied to the particular single device **(Banzhof: [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055])**.

ForcePoint LLC
EX-1002
Page134

As per claim 24, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices)**.

As per claim 25, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Cole: column 14, lines 28-65)**;

ForcePoint LLC
EX-1002
Page135

said potential vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith; said accurately identified vulnerability information is generated via a vulnerability scan operation **(Cole: column 17, lines 25-67)**;

said accurately identified vulnerability information identifies at least one accurately identified vulnerability; said accurately identified vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the accurately identified vulnerabilities **(Cole: column 17, lines 25-67)**;

said first device, said second device, and said third device are part of the same group; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch; said at least one configuration is capable of being utilized for identifying the at least one operating system or an application; said at least one configuration is identified utilizing information regarding the at least one operating system or an application; said at least one configuration is identified via user input in connection with at least one setting **(Cole: Fig. 1, column 14, lines 28-47, column 16, lines 39-67, column 18, line 56-column 19, line 50)**;

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that is capable of taking advantage of the at least one accurately identified vulnerability; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates

the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Banzhof: [0041], [0098])**;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Cohen: [0088])**;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Banzhof: [0041], [0098])**;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Banzhof: [0041], [0048]-[0052])**;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices; said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes

ForcePoint LLC
EX-1002
Page137

completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Banzhof: [0041], [0048]-[0052], [0057]-[0059])**;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first accurately identified vulnerability and utilizing a second one of the different occurrence mitigation actions for a second accurately identified vulnerability **(Banzhof: [0041], [0048]-[0052], [0057]-[0059])**;

said at least one accurately identified vulnerability is the at least one operating system **(Cole: column 17, lines 25-45)**;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Banzhof: [0041], [0048]-[0052], [0057]-[0059], Cole: column 17, lines 25-45)**;

one or more of said different occurrence mitigation actions is capable of being caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; one or more of said different

occurrence mitigation actions is capable of being caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; said different occurrence mitigation actions include different remediation actions; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Banzhof: [0041], [0048]-[0052], [0057]-[0059])**;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Cohen: [0055]-[0056], [0067], [0071], [0088])**;

said at least one accurately identified vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration **(Cole: column 17, lines 25-45)**;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software **(Cole: column 17, lines 25-45)**;

said determining that the plurality of devices is accurately identified as being vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration **(Cole: column 17, lines 25-45)**;

said non-transitory computer-readable media includes a single non-transitory computer readable medium; one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time **(Banzhof: [0048]-[0052])**;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation **(Banzhof: [0048]-[0052])**;

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch **(Banzhof: [0048]-[0052], Cohen: [0088])**;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component **(Banzhof: [0048]-[0052], [0098])**; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices **(Cole: column 17, lines 25-45)**.

As per claims 27 and 33, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation

ForcePoint LLC
EX-1002
Page140

actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055], [0100], [0107]-[0115]. Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically**

with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

As per claims 28 and 34, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter**

ForcePoint LLC
EX-1002
Page142

key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055]).

As per claims 29 and 35, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that different user input is capable of being received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is capable of resulting in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the**

firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Also, [0054]-[0055], [0100], [0107]-[0115]. Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

As per claims 30 and 36, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Banzhof: [0041]: using the central action pack module 28, a vulnerability resolution system administrator may construct one or more action packs suitable**

for use in remediating computer systems. Briefly, an action pack is comprised of a set of one or more remediations, each of which have been associated with one or more vulnerabilities, each of which, in turn, has been associated with one or more devices. [0050]: A remediation signature may, therefore, include a link to a vendor website where a patch or update is available for download. Similarly, an action to be undertaken as part of a remediation of a vulnerability of a computer system may include the download of the patch or update identified in a remediation signature. [0098]: For example, as part of the foregoing processes, a vulnerability in the portable computer 26C may be identified and mapped to a remediation signature. The remediation agent 163 may instead be instructed to use the firewall application 170 to close off the port under attack, to filter for specific identified elements, to filter for actions from specific identified processes, or otherwise be employed to temporarily or permanently block key access or filter key areas to mitigate the identified risk until a more elegant solution may be obtained. Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

As per claim 32, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation

ForcePoint LLC
EX-1002
Page145

actions is caused for different devices prior to the occurrence **(Banzhof: [0057] Once uploaded to the VFLASH server 20 by the central remediation server 12, a client remediation server such as the client remediation server 22 can download the action packs and/or the vulnerability/remediation entries from the VFLASH server 20. In this embodiment, a download is initiated, from the client administration console 25 by the network security administrator)**.

As per claim 37, Cole in view of Cohen and Banzhof teaches:

The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered**.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 6990660 to Moshir et al: Methods, systems, and configured storage media are provided for discovering software updates, discovering if a given computer can use

ForcePoint LLC
EX-1002
Page146

the software update, and then updating the computers with the software as needed automatically across a network without storing the updates on an intermediate machine within the network.

US 7152105 to McClure et al: A system and method provide comprehensive and highly automated testing of vulnerabilities to intrusion on a target network, including identification of operating system, identification of target network topology and target computers, identification of open target ports, assessment of vulnerabilities on target ports, active assessment of vulnerabilities based on information acquired from target computers, quantitative assessment of target network security and vulnerability, and hierarchical graphical representation of the target network, target computers, and vulnerabilities in a test report.

US 20030126472 to Carl Banzhof: A system and process for addressing computer security vulnerabilities.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI R HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on 8:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

ForcePoint LLC
EX-1002
Page147

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MADHURI R. HERZOG
Primary Examiner
Art Unit 2438

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1002
Page148

Notice of References Cited	Application/Control No. 15/608,978	Applicant(s)/Patent Under Reexamination Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6990660-B2	01-2006	Moshir; Sean	G06F8/62	709/223
*	B	US-7152105-B2	12-2006	McClure; Stuart C.	H04L41/12	709/224
*	C	US-20030126472-A1	07-2003	Banzhof, Carl E.	G06F21/577	726/25
*	D	US-20050193430-A1	09-2005	Cohen, Gideon	G06F21/577	726/25
*	E	US-7257630-B2	08-2007	Cole; David M.	G02B5/3083	709/224
*	F	US-20060101517-A1	05-2006	Banzhof; Carl E.	G06F21/577	726/25
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

CPC - Searched*		
Symbol	Date	Examiner
H04L 63/02$, 63/14$, 63/20$	06/19/2018	M.H
G06F 21/5$	06/19/2018	M.H

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search, Assignee search	06/19/2018	M.H
East search	06/19/2018	M.H

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page150

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/19/2018								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	-								
	19	-								
	20	-								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								
	37	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"14816931"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/14 15:38
S2	102	(determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or examin$6 or analy$4 or scan$4) with (vulnerabilit$4 or exploit$4) and (user or client or subscriber or customer or operator or administrator) with (choos$4 or select$4 or pick$4 or designat$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4) with (vulnerabilit$4 or exploit$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/14 16:24
S3	49	S2 and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4) with (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/14 16:26
S4	49	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/14 16:31
S5	732	(choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4) with (base$4 or depend$4 or type or kind or contingent) near5 (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 09:14
S6	179	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 09:15
S7	153	(choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4) with (base$4 or depend$4 or type or kind or contingent) near5 (operating system or os) and vulnerabilit$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 10:14
S8	15	"9117069"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 10:30
S9	32	"10882852"	US-PGPUB; USPAT; EPO; JPO;	ADJ	ON	2018/06/15 10:32

ForcePoint LLC
EX-1002
Page152

			DERWENT; IBM_TDB			
S10	22	"7353539"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 10:36
S11	155	"7257630"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 10:45
S12	42	"10050675"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 11:02
S13	3	"20030126472"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 11:04
S14	3	"20050235360"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 11:11
S15	3	"20050193430"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 11:11
S16	7	"09957673"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/06/15 12:00

EAST Search History (Interference)

< This search history is empty>

6/19/2018 1:07:23 PM
C:\Users\mherzog\Documents\EAST\Workspaces\App15608978.wsp

ForcePoint LLC
EX-1002
Page153

Bibliographic Data

Application No: 15/608,978

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /MADHURI R HERZOG/ (Examiner's Signature) (Initials)

Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/30/2017	726	2438	SP1P012C
RULE			

APPLICANTS

SecurityProfiling, LLC, Woodville, TX,

INVENTORS

Brett M. Oliphant Plano, TX, UNITED STATES

John P. Blignaut West Lafayette, IN, UNITED STATES

CONTINUING DATA

This application is a CON of 14816931 08/03/2015

14816931 is a CON of 14499230 09/28/2014 PAT 9100431

14499230 is a CIP of 14138014 12/21/2013 PAT 9117069

14138014 is a CON of 10882852 07/01/2004

10882852 has PRO of 60484085 07/01/2003

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

06/12/2017

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229
UNITED STATES

FILING FEE RECEIVED

$730

ForcePoint LLC
EX-1002
Page155

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION AND TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	15608978
Filing Date	30-May-2017
First Named Inventor	Brett Oliphant
Attorney Docket Number	SP1P012C
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
SecurityProfiling, LLC	100 %

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

14816931 filed on 08/03/2015

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9118711

9117069

9225686

8984644

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicants claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 44580

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Patrick Caldwell/
Name	Patrick Caldwell

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal	
Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		160

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15608978

Filing Date: 30-May-2017

Applicant/Patent under Reexamination: Oliphant

Electronic Terminal Disclaimer filed on July 24, 2018

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

ForcePoint LLC
EX-1002
Page161

Electronic Acknowledgement Receipt	
EFS ID:	33269714
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	24-JUL-2018
Filing Date:	30-MAY-2017
Time Stamp:	16:17:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	072518INTEFSW16171100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	37076 ef402b354f2a6b7cf1b1affa1379cccfd544353d	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30621 5cf524a7d36d8db198a1a8d82becf7a08835dbd2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	67697		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: July 24, 2018

AMENDMENT A

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 6/22/18, please enter the following amendments

C

ForcePoint LLC
EX-1002
Page164

Amendments to the Claims:

The listing of amended claims follows:

1.-20. (Cancelled)

21. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive ~~accurately identified~~first vulnerability information from at least one first data storage that is generated utilizing ~~potential~~second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said ~~accurately identified~~first vulnerability information generated utilizing the ~~potential~~second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the ~~potential~~second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the ~~accurately identified~~first vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices

ForcePoint LLC
EX-1002
Page165

for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

22. (Currently Amended) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is ~~capable of being~~ applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is ~~capable of being~~ applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device.

23. (Currently Amended) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that at least two options are provided including a firewall-type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is ~~capable of being~~ applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection

C

ForcePoint LLC
EX-1002
Page166

with a particular single device of the plurality of devices, the firewall-type option is ~~capable of being~~ applied to the particular single device.

24. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith.

25. (Cancelled)

26. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive ~~accurately identified~~first vulnerability information from at least one first data storage that is generated utilizing ~~potential~~second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said ~~accurately identified~~first vulnerability information generated utilizing the ~~potential~~second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one

C

ForcePoint LLC
EX-1002
Page167

configuration, utilizing the ~~potential~~second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the ~~accurately identified~~first vulnerability information; and

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

27. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page168

28. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

29. (Currently Amended) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that different user input is ~~capable of being~~permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input ~~is capable of resulting~~ results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page169

30. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

31. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive ~~accurately identified~~first vulnerability information from at least one first data storage that is generated utilizing ~~potential~~second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said ~~accurately identified~~first vulnerability information generated utilizing the ~~potential~~second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

ForcePoint LLC
EX-1002
Page170

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the ~~potential~~second vulnerability information that is used to identify the plurality of potential vulnerabilities;

display information that is based on the ~~accurately identified~~first vulnerability information;

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices;

wherein the at least one configuration involves at least one operating system.

32. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence.

33. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being caused at the first device in response to the occurrence, the utilization of

ForcePoint LLC
EX-1002
Page171

only a second occurrence mitigation action of the intrusion mitigation system-based occurrence mitigation type being caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being caused at the third device in response to the occurrence.

34. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

35. (Currently Amended) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that different user input ~~capable of being~~ is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input ~~is capable of resulting~~ results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user- completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion mitigation system-based occurrence mitigation type being completed at the second device in response to the occurrence, and both

ForcePoint LLC
EX-1002
Page172

the first occurrence mitigation action and the second occurrence mitigation action being completed at the third device in response to the occurrence.

36. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

37. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation.

C

ForcePoint LLC
EX-1002
Page173

38. (New) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence.

39. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only relevant occurrence mitigation actions are available for selection by the user.

40. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one accurately identified vulnerability.

41. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that different user input is allowed to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed

C

ForcePoint LLC
EX-1002
Page174

at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

42. (New) The non-transitory computer-readable media of Claim 41, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device.

43. (New) The non-transitory computer-readable media of Claim 41, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device.

44. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability.

C

ForcePoint LLC
EX-1002
Page175

45. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

determine the occurrence to have a first severity if it is determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence;

determine the occurrence to have a second severity if it determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is not susceptible to being taken advantage of by the occurrence; and

report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity.

46. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action.

47. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the

C

ForcePoint LLC
EX-1002
Page176

different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options.

48. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

49. (New) The non-transitory computer-readable media of Claim 48, wherein the instructions are configured such that the automatic application of the first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending

C

ForcePoint LLC
EX-1002
Page177

a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type includes sending a second signal to at least one component with intrusion prevention system functionality.

50. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences.

51. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one accurately identified vulnerability while there is no installation of a patch that removes the at least one accurately identified vulnerability.

52. (New) The non-transitory computer-readable media of Claim 21, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device; the determining that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine

ForcePoint LLC
EX-1002
Page178

whether a first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one second occurrence packet; and the allowing the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall-based occurrence mitigation type is completed by sending a first signal over at least one network to a first component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type is completed by sending a second signal to a second component with an intrusion prevention system type functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device.

53. (New) The non-transitory computer-readable media of Claim 52, wherein the instructions are configured such that at least one of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of:

ForcePoint LLC
EX-1002
Page179

receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said first vulnerability information is generated via a vulnerability scan operation;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

C

ForcePoint LLC
EX-1002
Page180

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said at least one accurately identified vulnerability includes the at least one operating system;

said actual vulnerabilities include the at least one accurately identified vulnerability;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which includes the at least one

ForcePoint LLC
EX-1002
Page181

operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one aspect of the at least one first occurrence packet involves at least one of a payload thereof or an IP address;

said at least one aspect of the at least one first occurrence packet is utilized to determine whether the first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, by utilizing the at least one aspect in connection with at least one of a cross-referencing operation or a look-up operation;

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action;

said first signal and thee second signal include at least one of response signals, or signals sent in response to a query signal;

C

ForcePoint LLC
EX-1002
Page182

said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality;

said second component with the intrusion prevention system type functionality includes at least one of an intrusion prevention system, an intrusion detection system with the intrusion prevention system type functionality, a gateway with the intrusion prevention system type functionality, a router with the intrusion prevention system type functionality, a sensor with the intrusion prevention system type functionality, or a multiple-security product system with the intrusion prevention system type functionality;

said preventing includes at least one of rejecting a request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or

said automatic response includes a real-time response.

54. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information identifies at least one actual vulnerability;

C

ForcePoint LLC
EX-1002
Page183

said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is utilized for identifying the at least one operating system or an application;

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the

C

ForcePoint LLC
EX-1002
Page184

occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said at least one actual vulnerability is the at least one operating system;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first

ForcePoint LLC
EX-1002
Page185

aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is actually vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

C

ForcePoint LLC
EX-1002
Page186

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

55. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused.

56. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence.

C

ForcePoint LLC
EX-1002
Page187

57. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence.

58. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

C

ForcePoint LLC
EX-1002
Page188

59. (New) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said second vulnerability information includes actual vulnerability information;

said second vulnerability information includes potential vulnerability information;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information identifies at least one accurately identified vulnerability;

said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the accurately identified vulnerabilities;

said first vulnerability information includes potential vulnerability information;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is utilized for identifying the at least one operating system or an application;

C

ForcePoint LLC
EX-1002
Page189

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions

ForcePoint LLC
EX-1002
Page190

and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first accurately identified vulnerability and utilizing a second one of the different occurrence mitigation actions for a second accurately identified vulnerability;

said at least one accurately identified vulnerability is the at least one operating system;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

ForcePoint LLC
EX-1002
Page191

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one accurately identified vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is accurately identified as being vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

C

ForcePoint LLC
EX-1002
Page192

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

C

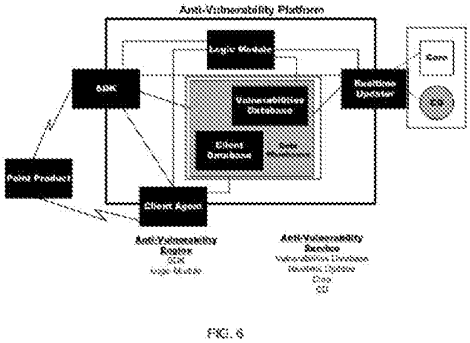
ForcePoint LLC
EX-1002
Page193

Remarks:

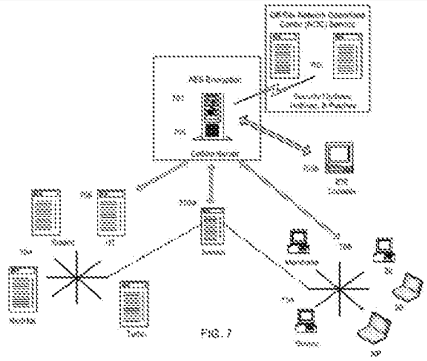
The claims have been clarified.

The claims are rejected on the ground of nonstatutory double patenting as being unpatentable over U.S. Patent No. 8984644, U.S. Patent No. 9225686, U.S. Patent No. 9117069, U.S. Patent No. 9118711, and Application Nos. 15/608981, and 14/816931. Such rejection is deemed avoided by virtue of the terminal disclaimers filed concurrently herewith.

Claims 21, 26, and 31 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner indicated that no support was found describing describing the procedure to determine accurately identified vulnerability information of a device based on device configuration and potential vulnerability information. Applicant respectfully disagrees. See Figs. 5B-12 and description thereof (with exemplary excerpts below-annotations/emphasis added). It should be also noted that the substance of such excerpts may also be found in U.S. App. No.: 60/484,085, filed July 1, 2003.

Claim Language	Exemplary Support
receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;	

ForcePoint LLC
EX-1002
Page194

	 "**Network operations center (NOC) Servers** periodically synchronize the **customers' servers** with the latest **vulnerability** and update data."" "technology may integrate with and enable network security products to intelligently reference and share information from the **same vulnerability data set**,"
said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;	"….automatically determines the update and dependency requirements for all computers on a network, based on their individual **operating systems**, **applications, and previously installed updates**…" "a product architect can integrate functionalities listed in the previous section to enable the scanner to access the logic engine and platform, and then have the intelligence to determine if the machine has **actual vulnerabilities**, remediate them, and verify policy compliance." "the platform enables network security products to share information via its proprietary logic engine to automatically **cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat**." "the platform may also remotely and proactively remediate vulnerabilities **by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed**. Then, the updates may be deployed, installed, and validated. ….

ForcePoint LLC
EX-1002
Page195

	The **same vulnerability data warehouse information** is shared with all products so that more intelligent actions may then be taken to mitigate complex threats. Still yet, **it may cross-reference the threat's identifier with the target's configuration**. The threat's CVE ID, or other identifier, and the destination IP address are fed into the logic engine **where it cross-references the threat with the machine's existing OS, application, and patch configuration profile**. **An answer is returned accurately indicating if the machine is vulnerable.** Thereby, minimizes erroneous, benign, and false positive data produced by each security product. **One embodiment identifies network vulnerabilities. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly**." "In 804, agents **accurately identifies OS, apps, and updates installed on each client by file versions and hashes**. In 805, **logic engine automatically determines which updates are needed on each client, taking into account OS, app, and update dependencies**. In 806, appropriate updates are automatically deployed, installed, and validated on each client." "As shown in 1104, agents are deployed to each client, **accurately identifying which OS, apps, and updates are installed**. In 1105, **the logic engine automatically determines which updates are needed to remediate the targeted machine, and may be remotely deployed from the IPS console**. In 1106, appropriate updates are remotely deployed, installed, and validated on each client." "Vulnerability scanners assess each machine on the network for vulnerabilities, and create lists of potential vulnerabilities to the system managers." "For example, if the malicious code has been written as a Windows based attack targeting a **Windows** vulnerability, is the Destination IP actually running **Windows**, or a UNIX variant? And, if Windows, is it vulnerable to the attack, or has it already been patched?"

ForcePoint LLC
EX-1002
Page196

It should be noted that such non-exhaustive exemplary support is set forth for illustrative purposes only, and such citations (and any context thereof) should not be construed as limiting to claims in any manner.

Claims 22, 23, 25, 29, and 35 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Such rejection is deemed avoided by virtue of the amendments made hereinabove.

Claims 21-37 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7257630 to Cole et al (hereinafter Cole), US 20050193430 to Cohen et al (hereinafter Cohen) and US 20060101517 to Banzhof et al (hereinafter Banzhof). In response, applicant respectfully notes that Banzhof has an earliest filing date of October 28, 2004, and the instant application claims priority to U.S. App. No.: 60/484,085 filed July 1, 2003. Thus, Banzhof is not prior art, and the above rejection is unfounded.

It is believed that all of the pending issues have been addressed. The claims are in condition for allowance. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, it should be noted that no claim is intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant the appropriate fees for the request for continued examination and the newly added claims. Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other

C

ForcePoint LLC
EX-1002
Page197

than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-4964 (Order No. SP1P012C).

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

Respectfully submitted,



Dated: 24 Jul 2018

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

C

ForcePoint LLC
EX-1002
Page198

Electronic Patent Application Fee Transmittal					
Application Number:	15608978				
Filing Date:	30-May-2017				
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION				
First Named Inventor/Applicant Name:	Brett M. Oliphant				
Filer:	Patrick Edgar Caldwell				
Attorney Docket Number:	SP1P012C				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
CLAIMS IN EXCESS OF 20		2202	18	50	900
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**900**

Electronic Acknowledgement Receipt	
EFS ID:	33269477
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	24-JUL-2018
Filing Date:	30-MAY-2017
Time Stamp:	18:47:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$900
RAM confirmation Number	072518INTEFSW18475700
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	SP1P012C_AmendmentA_vF_24-Jul-2018.pdf	269563 0ff571f9766f63dc4e868a37e11d068393a3569c	no	35
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30587 117fc9d3c21a438c830abf65b528f8e654d29243	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	300150		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/608,978	Filing Date 05/30/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	07/24/2018	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 38	Minus	** 20	= 18		x $50 =	900
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	900

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	Tracey M Young
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Oliphant et al. Application No.: 15/608,978 Filed: 5/30/2017 For: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Confirmation No.: 9647 Examiner: HERZOG, Madhuri R. Art Unit: 2438 Atty. Docket No.: SP1P012C Date: 10/25/2018

Please correct the Applicant Information as follows:

APPLICANT INFORMATION

Applicant Type::	Assignee
Organization Name::	SecurityProfiling, LLC
Mailing Address::	~~318 West Dogwood~~ 1919 S Shiloh Rd.
City::	~~Woodville~~ Garland
State::	TX
Postal Code::	~~75979~~ 75042
Country::	US

SIGNATURE:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Respectfully submitted,



Dated: 25 Oct 2018

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page204

Electronic Acknowledgement Receipt	
EFS ID:	34121815
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	25-OCT-2018
Filing Date:	30-MAY-2017
Time Stamp:	21:27:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	SP1P012C_Supp_ADS_vF_25-Oct-2018.pdf	28419 d086d9f436252c6751c8ee12d1edb1f346484670	no	1

Warnings:

Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	28419

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 11/05/2018

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER	
HERZOG, MADHURI R	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
11/05/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

Office Action Summary	**Application No.** 15/608,978	**Applicant(s)** Oliphant et al.	
	Examiner MADHURI R HERZOG	**Art Unit** 2438	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 07/24/2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 21-24 and 26-59 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 21-24 and 26-59 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The following is a Final Office action in response to communications received 07/24/2018.

Terminal Disclaimer

3. The terminal disclaimer filed on 07/24/2018 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **any patent granted on Application Number 14/816931 and Patent Numbers 9118711, 9117069, 9225686 and 8984644** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Amendment

4. Claims 25 has been cancelled. Claims 38-59 have been newly added.

5. Claims 21-23, 26, 29, 31 and 35 have been amended.

6. Examiner's provisional double patenting rejection of the claims over claims of 14/816931 and double patenting rejection of the claims over claims of US 9118711, US 9117069, US 9225686 and US 8984644 has been withdrawn in light of the terminal disclaimer filed by the applicants.

ForcePoint LLC
EX-1002
Page209

7. Examiner's rejection of claims 21, 26 and 31 under 35 U.S C 112(a) or 35 U.S.C 112, first paragraph (pre-AIA) has been withdrawn in light of the applicant's amendments to the claims.

8. Examiner's rejection of claims 22, 23, 25, 29 and 35 under 35 U.S C 112(b) or 35 U.S.C 112, second paragraph (pre-AIA) has been withdrawn in light of the applicant's amendments to the claims.

9. Applicant's arguments with respect to claims 21-37 have been considered but are moot in view of the new grounds of rejection presented in the current rejection.

Double Patenting

10. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

ForcePoint LLC
EX-1002
Page210

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

11. Claims 21-24 and 26-58 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims 21-46 of copending Application No. 15/608981 (reference application). Although the claims at issue are not identical, they are not patentably distinct from each other because:

ForcePoint LLC
EX-1002
Page211

Claim 21 of the instant application: 21. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities; identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; wherein the at least one configuration involves at least one operating system.

Is analogous to:

ForcePoint LLC
EX-1002
Page212

Claim 21 of Application No. 15/608981: 21. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including: at least one first potential vulnerability, and at least one second potential vulnerability; said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities; identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; wherein the at least one configuration involves at least one operating system.

ForcePoint LLC
EX-1002
Page213

Similarly, the rest of the dependent and independent claims of the instant application are analogous to the rest of the dependent and independent claims of Application No. 15/608981.

This is a provisional nonstatutory double patenting rejection because the patentably indistinct claims have not in fact been patented.

Claim Rejections - 35 USC § 112

12. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 21, 26 and 31 rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claim 21 has been amended to recite first vulnerability information and second vulnerability information. However, the claim also recites accurately identified vulnerability and potential vulnerability. It is unclear whether these phrases are the same as first and second vulnerabilities or different. Claims 26 and 31 have similar issues.

14. Also, claim 21 recites: "determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities". The applicant cited paragraphs showing support for

ForcePoint LLC
EX-1002
Page214

this limitation. However, the specification of the instant application and parent applications show support for determining whether a device is vulnerable to a vulnerability based on configuration and vulnerability information shared and stored amongst various devices. The specifications do not cite determining whether a device is vulnerable based on potential vulnerabilities. The phrase "potential" indicates that a vulnerability has the potential to a vulnerability but not guaranteed to be a vulnerability. As indicated above, the specifications show support for determining that a device is vulnerable to a vulnerability based on vulnerabilities shared amongst various device but does not show proper support for determining that a device is vulnerable to a vulnerability based on "potential vulnerabilities". Claims 26 and 31 have similar issues.

Claim Rejections - 35 USC § 103

15. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 21-24, 26, 27, 31-33, 37-2, 45, 46, 50-52 and 55-57 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over prior art of record US 7257630 to Cole et al (hereinafter Cole), prior art of record US 20050193430 to Cohen et al (hereinafter Cohen) and US 6550012 to Villa et al (hereinafter Villa).

ForcePoint LLC
EX-1002
Page215

As per claims 21 and 26, Cole teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: As described in more detail below, in the vulnerability assessment routine 364, the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine whether the ports of the target computers exhibit the potential vulnerabilities. The method uses information stored in a known vulnerability database 366 to select the vulnerability scripts to execute for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database 344)**;

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential

ForcePoint LLC
EX-1002
Page216

vulnerabilities **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30)**;

wherein the at least one configuration involves at least one operating system **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**.

Cole does not teach: identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based

ForcePoint LLC
EX-1002
Page217

occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. However, Cohen teaches:

identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information **(Cohen: [0067]: FIG. 3 is a flow diagram showing a method of verifying actual vulnerabilities in a computer network in accordance with one embodiment of the present invention. To find raw vulnerabilities which could be exploited, the information discovery agents scan the network from the perspective of an attacker by starting attacks, but stopping before too much damage is done. Packets of data are sent to each network device and any responses received back from the network devices are interpreted to determine whether a raw vulnerability exists. The information discovery agent would send packets containing a query command for the BIND server on a network to return its version number. If the BIND server returns a version number which is known to be vulnerable to attacks, the information discovery agent would report the raw vulnerability. [0071]: As such, in some embodiments, the logic can specify pre-conditions for exploitation of vulnerabilities. [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers)**; and

ForcePoint LLC
EX-1002
Page218

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Cohen in the invention of Cole to include identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately

ForcePoint LLC
EX-1002
Page219

identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to conduct security assessments automatically in a computer network (Cohen: [0010]).

Cole in view of Cohen teaches intrusion prevention system-based occurrence mitigation type but does not teach a firewall-based occurrence mitigation type. However, Villa teaches

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Villa: column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine))**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Villa in the invention of Cole in view of Cohen to include allow selective utilization of different occurrence mitigation

ForcePoint LLC
EX-1002
Page220

actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to provide automated or proactive network security (Villa: column 3, lines 20-22).

As per claim 31, Cole teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: As described in more detail below, in the vulnerability assessment routine 364, the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine whether the ports of the target computers exhibit the potential vulnerabilities. The method uses information stored in a known vulnerability database 366 to select the vulnerability scripts to execute for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database 344)**;

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of

ForcePoint LLC
EX-1002
Page221

devices including a first device, a second device, and a third device **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30)**;

display information that is based on the first vulnerability information **(Cole: column 68, lines 58-67: Thus, in one embodiment of the present invention, the reports engine produces (1) a dynamic graphical display representing the network topology, the target computers found, and the vulnerabilities found**

throughout the target network; (2) a comprehensive list of target computers, vulnerabilities found, and vulnerability explanations);

wherein the at least one configuration involves at least one operating system **(Cole: column 16, lines 39-67: the method proceeds to an operating system (OS) identification routine 350 wherein the method determines the type and version of operating system present on each of the live computers having open ports)**.

Cole does not teach: cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices. However, Cohen teaches:

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In**

ForcePoint LLC
EX-1002
Page223

some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Cohen in the invention of Cole to include cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices. The motivation to do so would be to conduct security assessments automatically in a computer network (Cohen: [0010]).

Cole in view of Cohen teaches a intrusion mitigation system-based occurrence mitigation type but does not teach a firewall-based occurrence mitigation type. However, Villa teaches:

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Villa: column**

**ForcePoint LLC
EX-1002
Page224**

12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine)).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Villa in the invention of Cole in view of Cohen to include cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices. The motivation to do so would be to provide automated or proactive network security (Villa: column 3, lines 20-22).

As per claim 22, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention-type option for preventing a connection request; the instructions are

ForcePoint LLC
EX-1002
Page225

configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 7, lines 55-67: System 220 includes a user interface (UI) 260, preferably a Graphical User Interface (GUI), for receiving user commands and data. These inputs, in turn, may be acted upon by the system 100 in accordance with instructions from OS module 240, windows shell 250, and/or client application module(s) 245. Column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new**

ForcePoint LLC
EX-1002
Page226

certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. Here, the network is configured at the outset (e.g., by a system administrator) to specify which components may participate in the secured communication process. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine)).

As per claim 23, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that at least two options are provided including a firewall-type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular

ForcePoint LLC
EX-1002
Page227

single device of the plurality of devices, the firewall-type option is applied to the particular single device **(Villa: column 7, lines 55-67: System 220 includes a user interface (UI) 260, preferably a Graphical User Interface (GUI), for receiving user commands and data. These inputs, in turn, may be acted upon by the system 100 in accordance with instructions from OS module 240, windows shell 250, and/or client application module(s) 245. Column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. Here, the network is configured at the outset (e.g., by a system administrator) to specify which components may participate in the secured communication process. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine))**.

As per claim 24, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid

ForcePoint LLC
EX-1002
Page228

false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. Villa: column 7, lines 55-67: System 220 includes a user interface (UI) 260, preferably a Graphical User Interface (GUI), for receiving user commands and data. These inputs, in turn, may be acted upon by the system 100 in accordance with instructions from OS module 240, windows shell 250, and/or client application module(s) 245. Column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. Here, the network is configured at the outset (e.g., by a system administrator) to specify which components may participate in the secured communication process)**.

As per claims 27, 33 and 41, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation

ForcePoint LLC
EX-1002
Page229

actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence **(Villa: Column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. Here, the network is configured at the outset (e.g., by a system administrator) to specify which components may participate in the secured communication process. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine). Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

ForcePoint LLC
EX-1002
Page230

As per claims 32 and 38, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence **(Villa: column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available)**.

As per claim 37, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

As per claim 39, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only

ForcePoint LLC
EX-1002
Page231

relevant occurrence mitigation actions are available for selection by the user **(Cole: column 68, lines 58-67: Thus, in one embodiment of the present invention, the reports engine produces (1) a dynamic graphical display representing the network topology, the target computers found, and the vulnerabilities found throughout the target network; (2) a comprehensive list of target computers, vulnerabilities found, and vulnerability explanations. Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available**).

As per claim 40, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one accurately identified vulnerability **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability**

ForcePoint LLC
EX-1002
Page232

checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340).

As per claim 42, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 41, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device **(Villa: column 7, lines 55-67: System 220 includes a user interface (UI) 260, preferably a Graphical User Interface (GUI), for receiving user commands and data. These inputs, in turn, may be acted upon by the system 100 in accordance with instructions from OS module 240, windows shell 250, and/or client application module(s) 245. Column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

ForcePoint LLC
EX-1002
Page233

As per claim 45, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: determine the occurrence to have a first severity if it is determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence; determine the occurrence to have a second severity if it determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is not susceptible to being taken advantage of by the occurrence; and report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity **(Cohen: [0012], [0056] The probability of an attack taking place is combined with the consequences data to rank the vulnerabilities according to actual risks presented and present fixes for the vulnerabilities, step 140. In some embodiments, the system also ranks the risk level of threats and attacks, as well as the risks of business applications and IT infrastructure. In some embodiments, risk takes into account the degree or magnitude of potential damage from a particular attack as well as a probability of such an attack. Vulnerabilities with high consequences data and a high probability of being executed will rank higher in terms than vulnerabilities with lower consequences data and lower probability of being executed. [0082]: The present system permits prioritization of vulnerabilities by performing risk mitigation analysis of the vulnerabilities. For example, some vulnerabilities listed in the report such as the web server 246 and**

ForcePoint LLC
EX-1002
Page234

248 NetBios vulnerability and the administration server 254 finger vulnerability are not used in any attacks since these protocols are blocked by the firewalls 234 and 240. Fixes for these vulnerabilities can thus be put off until a later date).

As per claim 46, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 7, lines 55-67, column 11, lines 30-50 and column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. Here, the network is configured at the outset (e.g., by a system administrator) to**

ForcePoint LLC
EX-1002
Page235

specify which components may participate in the secured communication process. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine)).

As per claim 50, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 7, lines 55-67, column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct**

ForcePoint LLC
EX-1002
Page236

any system vulnerabilities, when that person is available. Also, Column 12, lines 30-67).

As per claim 51, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one accurately identified vulnerability while there is no installation of a patch that removes the at least one accurately identified vulnerability **(Villa: column 7, lines 55-67, column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available)**.

As per claim 52, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device **(Cole: column 17, lines 25-67, Cohen: [0088])**; the determining that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine whether a first actual vulnerability of the first device

ForcePoint LLC
EX-1002
Page237

identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one second occurrence packet **(Cole: column 17, lines 25-67, Cohen: [0088])**; and the allowing the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed by sending a first signal over at least one network to a first component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device **(Cohen: [0088], Villa: column 12, lines 30-67)**; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type is completed by sending a second signal to a second component with an intrusion prevention system type functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device **(Cohen: [0088], Villa: column 12, lines 30-67)**.

ForcePoint LLC
EX-1002
Page238

As per claim 55, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused **(Cole: column 17, lines 25-67: In one embodiment, the vulnerability assessment routine 364 preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine 350 and service discovery routine 340. the active assessment routine 365 uses information collected from target computers in the vulnerability assessment routine 364 to execute further vulnerability scripts to open ports of the live target computers. Specifically, the active assessment routine 365 reuses known vulnerabilities and information collected from target computers to continue to determine whether the ports of the target computers exhibit potential vulnerabilities, using information from the known vulnerability database 366 and information collected in the target computer database 344. Also, column 41, lines 7-30; Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise**

ForcePoint LLC
EX-1002
Page239

taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

As per claim 56, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

As per claim 57, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system- based occurrence mitigation type being selectively caused at the

ForcePoint LLC
EX-1002
Page240

second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence **(Cohen: [0088]: For example, an IDS system might issue an alert that it has detected network traffic to a particular host that appears to be trying to exploit a vulnerability known to affect IIS servers. In some embodiments, the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 12, lines 30-67: Upon receipt at the EO of a certogram reporting the problem, the EO may employ the Active Security Layer 350 to create a new certogram informing the actor (e.g., firewall) of detection of the network vulnerability and do so in an authenticated manner. The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine))**.

18. Claims 28, 29, 30, 34-36, 43, 44, 47-49, 53, 54, 58 and 59 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Cole in view of Cohen and Villa as applied to claim 21, 26 and 31 above, and further in view of prior art of record US 20030126472 to Carl Banzhof (hereinafter Banzhof).

ForcePoint LLC
EX-1002
Page241

As per claims 28, 34 and 58, Cole in view of Cohen and Villa does not teach receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Banzhof teaches:

receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Banzhof: [0024]: security or IT personnel via the server, could select which remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities. Also, [0028]-[0029])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based

ForcePoint LLC
EX-1002
Page242

on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claims 29 and 35, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence **(Villa: Column 12, lines 30-67: The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine). Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system**

ForcePoint LLC
EX-1002
Page243

measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

Cole in view of Cohen and Villa does not explicitly teach: wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions. However, Banzhof teaches:

wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions **(Banzhof: [0024]: security or IT personnel via the server, could select which remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities. Also, [0028]-[0029])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions. The motivation to do so would be to provide for a more automated and managed way to

ForcePoint LLC
EX-1002
Page244

remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claims 30 and 36, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Villa: column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Column 12, lines 30-67: The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine). Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing,**

ForcePoint LLC
EX-1002
Page245

defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered).

Cole in view of Cohen and Villa does not explicitly teach: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface and receive a second user input selecting a second one of the options, utilizing the at least one user interface. However, Banzhof teaches:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface and receive a second user input selecting a second one of the options, utilizing the at least one user interface **(Banzhof: [0024]: security or IT personnel via the server, could select which remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities. Also, [0028]-[0029])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface

ForcePoint LLC
EX-1002
Page246

and receive a second user input selecting a second one of the options, utilizing the at least one user interface. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claim 43, Cole in view of Cohen and Villa does not teach: wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. However, Banzhof teaches:

wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device **(Banzhof: [0031]: In box 86, the client user, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability does not pose a sufficient security risk, the remediation signature is deemed too**

risky, etc. [0032]: If the remediation is not deemed successful, either because it did not resolve the identified vulnerabilities as evidenced by an additional security scan of the client computer, or because the remediation actions had unintended deleterious effects, etc., then the remediation can be rolled back or undone and the remediation process can be repeated as indicated in box 99).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claim 44, Cole in view of Cohen and Banzhof does not teach: wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability. However, Banzhof teaches:

ForcePoint LLC
EX-1002
Page248

wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability **(Banzhof: [0031]: In box 86, the client user, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Generally, the selection is made by reviewing the information regarding vulnerabilities, proposed signatures, and profiles. The selection and review may be made for each computer or by vulnerability. Once the user has selectively managed which vulnerabilities will be remediated, the user can then select which computers will be approved to receive remediation in box 87. In box 88, the proposed remediation is analyzed to determine which remediation signatures will be required)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability. The motivation to do so would be to provide for a more automated and managed way to remediate

ForcePoint LLC
EX-1002
Page249

security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claim 47, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options **(Villa: Column 12, lines 30-67: The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine). Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered)**.

ForcePoint LLC
EX-1002
Page250

Cole in view of Cohen and Villa does not explicitly teach: multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence. However, Banzhof teaches:

multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence **(Banzhof: [0024]: security or IT personnel via the server, could select which remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities. Also, [0028]-[0029])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence. The motivation to do so would be

ForcePoint LLC
EX-1002
Page251

to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claim 48, Cole in view of Cohen and Villa teaches firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Banzhof teaches:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Banzhof: [0024]: security or IT personnel via the server, could select which**

ForcePoint LLC
EX-1002
Page252

remediation signatures should be deployed to each client computer 26, or which vulnerabilities should or should not be addressed. In addition, vulnerability resolution can be managed by scheduling the various resolution events. For instance, when and how often the client computers 26 are scanned for vulnerabilities can be scheduled, as well as the timing of the deployment of the remediation signatures to address those vulnerabilities. Also, [0028]-[0029]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claim 49, Cole in view of Cohen, Villa and Banzhof teaches:

The non-transitory computer-readable media of Claim 48, wherein the instructions are configured such that the automatic application of the first one of the

ForcePoint LLC
EX-1002
Page253

different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type includes sending a second signal to at least one component with intrusion prevention system functionality **(Cohen: [0088]: the system is also configured to control and instruct intrusion network and security system measures such as intrusion detection systems, and other devices automatically with respect to preventing, defending, or otherwise taking steps against attacks, exploits, and other activities based upon the raw vulnerabilities discovered. Villa: column 7, lines 55-67, column 11, lines 30-50: As a result, its primary use is to provide reports to an IT worker who must then manually correct any system vulnerabilities, when that person is available. Column 12, lines 30-67: The firewall (actor), assured of the authenticity of the message, may create a new rule on-the-fly to address the vulnerability. Thus for the example of a writeable FTP directory, the firewall may create a rule specifically handling the vulnerability (e.g., by blocking access to a specific port or machine))**.

As per claim 53, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 52, wherein the instructions are configured such that at least one of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Cole: column 14, lines 28-65)**; said second vulnerability

ForcePoint LLC
EX-1002
Page254

information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith; said first vulnerability information is generated via a vulnerability scan operation **(Cole: column 17, lines 25-67)**; said first device, said second device, and said third device are part of the same group; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch; said at least one configuration is identified via user input in connection with at least one setting **(Cole: Fig. 1, column 14, lines 28-47, column 16, lines 39-67, column 18, line 56-column 19, line 50)**; said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability **(Cohen: [0088])**; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Villa: column 12, lines 30-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Cohen: [0088])**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Villa: column 12, lines 30-67)**; said

ForcePoint LLC
EX-1002
Page255

preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said at least one accurately identified vulnerability includes the at least one operating system **(Cole: column 17, lines 25-45)**; said actual

ForcePoint LLC
EX-1002
Page256

vulnerabilities include the at least one accurately identified vulnerability **(Cole: Fig. 1, column 14, lines 28-47, column 16, lines 39-67, column 18, line 56-column 19, line 50)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which includes the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Villa: column 4, lines 33-50, column 12, lines 30-67, Cole: column 17, lines 25-45)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; said different occurrence mitigation actions include different remediation actions; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack; said at least one aspect of the at least one first occurrence packet involves at least one of a payload thereof or an IP address **(Cohen: [0055]-[0056], [0067], [0071], [0088])**; said at least one aspect of the at least one first occurrence packet is utilized to determine whether the first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken

ForcePoint LLC
EX-1002
Page257

advantage of by the at least one first occurrence packet, by utilizing the at least one aspect in connection with at least one of a cross-referencing operation or a look-up operation **(Cole: column 17, lines 25-45, Cohen: [0055]-[0056], [0067], [0071], [0088])**; said first signal and the second signal include at least one of response signals, or signals sent in response to a query signal; said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality **(Villa: column 4, lines 33-50, column 11, lines 30-50 and column 12, lines 30-67)**; said second component with the intrusion prevention system type functionality includes at least one of an intrusion prevention system, an intrusion detection system with the intrusion prevention system type functionality, a gateway with the intrusion prevention system type functionality, a router with the intrusion prevention system type functionality, a sensor with the intrusion prevention system type functionality, or a multiple-security product system with the intrusion prevention system type functionality **(Cole: column 17, lines 25-45)**; said preventing includes at least one of rejecting a request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or said automatic response includes a real-time response **(Cohen: [0082]-[0083], Villa: column 12, lines 30-67)**.

Cole in view of Cohen and Villa does not explicitly teach: said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. However, Banzhof teaches:

ForcePoint LLC
EX-1002
Page258

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action **(Banzhof: [0024], [0028]-[0029])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

As per claims 54 and 59, Cole in view of Cohen and Villa teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Cole: column 14, lines 28-65)**; said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith; said first vulnerability information is generated via a vulnerability scan operation **(Cole: column 17, lines 25-67)**; said first vulnerability information identifies at least one actual vulnerability; said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities **(Cole: column 17, lines 25-67)**; said first

ForcePoint LLC
EX-1002
Page259

device, said second device, and said third device are part of the same group; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch; said at least one configuration is utilized for identifying the at least one operating system or an application; said at least one configuration is identified utilizing information regarding the at least one operating system or an application; said at least one configuration is identified via user input in connection with at least one setting **(Cole: Fig. 1, column 14, lines 28-47, column 16, lines 39-67, column 18, line 56-column 19, line 50)**; said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Villa: column 12, lines 30-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Cohen: [0088])**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Villa: column 12, lines 30-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the

ForcePoint LLC
EX-1002
Page260

plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said at least one actual vulnerability is the at least one operating system **(Cole: column 17, lines 25-45)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation

ForcePoint LLC
EX-1002
Page261

actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Villa: column 4, lines 33-50, column 12, lines 30-67, Cole: column 17, lines 25-45)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; said different occurrence mitigation actions include different remediation actions; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Cohen: [0055]-[0056], [0067], [0071], [0088])**; said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration **(Cole: column 17, lines 25-45)**; said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software **(Cole: column 17, lines 25-45)**; said determining that the plurality of devices is actually vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration

ForcePoint LLC
EX-1002
Page262

with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration **(Cole: column 17, lines 25-45)**; said non-transitory computer-readable media includes a single non-transitory computer readable medium; one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time **(Villa: column 4, lines 33-50, column 11, lines 30-50 and column 12, lines 30-67)**; one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation **(Villa: column 4, lines 33-50, column 12, lines 30-67)**; and wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices **(Cole: column 17, lines 25-45)**.

Cole in view of Cohen and Villa does not explicitly teach: one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch; one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component. However, Banzhof teaches:

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to

ForcePoint LLC
EX-1002
Page263

deploy a patch; one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component **(Banzhof: [0020]: patch installation)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Cole in view of Cohen and Villa to include one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch; one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

Conclusion

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

ForcePoint LLC
EX-1002
Page264

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI R HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on 8:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ForcePoint LLC
EX-1002
Page265

MADHURI R. HERZOG
Primary Examiner
Art Unit 2438

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1002
Page266

Notice of References Cited	Application/Control No. 15/608,978	Applicant(s)/Patent Under Reexamination Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6550012-B1	04-2003	Villa; Emilio	H04L63/0218	713/168
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

CPC - Searched*		
Symbol	Date	Examiner
H04L 63/02$, 63/14$, 63/20$	10/30/2018	M.H
G06F 21/5$	10/30/2018	M.H

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search, Assignee search	10/30/2018	M.H
East search	10/30/2018	M.H

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page268

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018							
	1	-	-							
	2	-	-							
	3	-	-							
	4	-	-							
	5	-	-							
	6	-	-							
	7	-	-							
	8	-	-							
	9	-	-							
	10	-	-							
	11	-	-							
	12	-	-							
	13	-	-							
	14	-	-							
	15	-	-							
	16	-	-							
	17	-	-							
	18	-	-							
	19	-	-							
	20	-	-							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	-							
	26	✓	✓							
	27	✓	✓							
	28	✓	✓							
	29	✓	✓							
	30	✓	✓							
	31	✓	✓							
	32	✓	✓							
	33	✓	✓							
	34	✓	✓							
	35	✓	✓							
	36	✓	✓							
	37	✓	✓							
	38		✓							
	39		✓							
	40		✓							
	41		✓							
	42		✓							

ForcePoint LLC
EX-1002
Page269

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018							
	43		✓							
	44		✓							
	45		✓							
	46		✓							
	47		✓							
	48		✓							
	49		✓							
	50		✓							
	51		✓							
	52		✓							
	53		✓							
	54		✓							
	55		✓							
	56		✓							
	57		✓							
	58		✓							
	59		✓							

ForcePoint LLC
EX-1002
Page270

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S17	72	(choos$4 or select$4 or pick$4 or designat$4 or inform or informing) with firewall with vulnerabilit$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/26 12:51
L3	59	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and L2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/30 11:52
L2	72	(choos$4 or select$4 or pick$4 or designat$4 or inform or informing) with firewall with vulnerabilit$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2018/10/30 11:52

EAST Search History (Interference)

< This search history is empty>

10/ 30/ 2018 11:53:02 AM
C:\ Users\ mherzog\ Documents\ EAST\ Workspaces\ App15608978.wsp

ForcePoint LLC
EX-1002
Page271

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		SP1P012C	15/608,978
		Inventor: Brett M. Oliphant	Confirmation Number: 9647
		Filing Date: 05/30/2017	Group Art Unit: 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	A	Action Summary for US Pat Appl No 14834102 dated 08/24/2918
	B	Action Summary for US Pat Appl No 15608981 dated 11-05-2018
	C	Action Summary for US Pat Appl No 15608983 dated 09-11-2018

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	
Name/Print	Brian Owens	Registration Number	55517

Electronic Patent Application Fee Transmittal	
Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**120**

Electronic Acknowledgement Receipt	
EFS ID:	34315014
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	14-NOV-2018
Filing Date:	30-MAY-2017
Time Stamp:	21:35:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$120
RAM confirmation Number	111518INTEFSW21354900
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	SP1P012C_IDS_XMTL_vF_14-Nov-2018.pdf	55666 26567e4bb138b6e405e07ebd178e33822c0b9f3e	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	SP1P012C_IDS_1449_vF_14-Nov-2018.pdf	56499 879630db2422a8af9a6e7c754c6f782003fae877	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	NPL_20181113.pdf	517034 892359a9092f0a405760599751fbf247dba4e199	no	76
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30456 e391ea23299b3a90258e8f0281c89c03b8714cb5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	659655		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 2017-05-30	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: Nov 14, 2018

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

ForcePoint LLC
EX-1002
Page279

Additionally, related patent US8266699, is the subject of inter partes review (IPR No. 2017-02191), where a request for adverse judgment was recently filed in such IPR No. 2017-02191 due to Claim 7 being disclaimed from related patent US8266699.

This Information Disclosure Statement is being filed after the mailing date of a final Office Action. Accordingly, applicants are including payment in the amount of $120.00 for the fee due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-4964 (Order No. SP1P012C).

Respectfully submitted,



Dated: 14 Nov 2018

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	15608978
Filing Date	30-May-2017
First Named Inventor	Brett Oliphant
Attorney Docket Number	SP1P012C
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
SecurityProfiling, LLC	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

15608981 filed on 05/30/2017

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

◯ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

◉ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 44580 ◯ A sole inventor ◯ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ◯ A joint inventor; all of whom are signing this request	
Signature	/Patrick Caldwell/
Name	Patrick Caldwell

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15608978

Filing Date: 30-May-2017

Applicant/Patent under Reexamination: Oliphant

Electronic Terminal Disclaimer filed on February 21, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

ForcePoint LLC
EX-1002
Page283

Electronic Acknowledgement Receipt	
EFS ID:	35219717
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	21-FEB-2019
Filing Date:	30-MAY-2017
Time Stamp:	22:22:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	32466 7bc3a6f232a40703b92bc903b8198cfe4a55e88d	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	32466

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15608978	Filing Date	2017-05-30	Docket Number (if applicable)	SP1P012C	Art Unit	2438
First Named Inventor	Brett M. Oliphant			Examiner Name	HERZOG, MADHURI R		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☒ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504964

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-02-21
Name	Patrick Caldwell	Registration Number	44580

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

DECLARATION OF JOHN BLIGNAUT UNDER 37 CFR § 1.131

I, John Blignaut, declare the following:

1. I am John Blignaut, member of SecurityProfiling, LLC ("Assignee"), the assignee of the patent application identified above (the "Application"), and an inventor named on the Application.

2. I have personal knowledge of the facts set forth in this Declaration regarding the conception and reduction to practice of the invention described and claimed in the Application.

3. The invention disclosed and claimed in the Application (the "Claimed Invention") was conceived of and actually reduced to practice before October 1, 2002 (the earliest effective date of US 20050193430 to Cohen, the "Reference Date").

C

ForcePoint LLC
EX-1002
Page289

4. The Claimed Invention was implemented with a system architecture that is reflected in the SDK White Paper attached as Annex A to this Declaration. The SDK White Paper documents the Software Development Kit (SDK) that was developed to allow application developers to access the database of vulnerability, device status, and remediation information that was eventually distributed under the trade name "AntiVulnerability Technology." I personally participated in development of that SDK White Paper and commercialization of products embodying the invention. The version of the SDK White Paper attached as Annex A was created on September 27, 2002, as a business record created in the ordinary course of business. The metadata in the electronic document reflects this date.

5. A working version of a system implementing the Claimed Invention was implemented before the Reference Date. Annex A reflects a system that was actually operational as of September 27, 2002, which is not antedated by the Reference Date.

7. As evidenced in Annex B, the Claimed Invention was conceived of and actually reduced to practice before Reference Date.

8. I provide these statements under penalty of perjury pursuant to 18 U.S.C. §1001.

John Blignaut

2.20.2019
Date

ForcePoint LLC
EX-1002
Page290

Anti-Vulnerability™

Software Development Kit (SDK)

White Paper

Version 1.0

The Intelligent Network Security Integration Platform

PATENT OWNER EXHIBIT
2014

SecurityProfiling Inc.
839 Main St., Suite 405
Lafayette, IN 47901
Toll Free: 888.645.3676
Phone: 765.420.7227
Fax: 765.420.9256

www.securityprofiling.com

Table of Contents

Table of Graphics 1

Executive Summary 3

What is the SDK and Anti-Vulnerability Platform? 5

Market Requirements 5

Solution 9

Functionalities Integrated with the SDK 10

1. Group Management Functions
2. Client Management Functions
3. Hot Fix Management Functions
4. Polling Functions
5. Vulnerability Query Functions
6. Conversion Functions

SDK Applications - Example Product Integration 3

1. Patch Deployment
2. Intrusion Detection System
3. Scanner
4. Firewall
5. Vulnerability Management
6. Mulitple Products: IDS, scanner, and firewall, and Vulnerability Managment
7. Client Security

Technical Description 21

Conclusion 24

Appendix I – List of Functionalities Integrated with the SDK 25

Appendix II – About SecurityProfiling 26

SCP0052201
ForcePoint LLC
EX-1002
Page292

Table of Graphics

Figure 1 SDK and Platform Overview Diagram 7

Figure 2 Platform Component Diagram 7

Figure 3 Functionality Query Flow Chart 7

SCP0052202
ForcePoint LLC
EX-1002
Page293
C

Executive Summary

What is the SDK and Anti-Vulnerability Platform?

The SDK was designed to be a simple integration pathway to the back-end Anti-Vulnerability platform - consisting of a logic engine and vulnerability data warehouse. It will enable any network security product such as an IDS, scanner, or firewall to intelligently reference and share the same vulnerability data set, and provide complete vulnerability remediation functionalities. Thereby, improving system accuracy and efficiencies, minimizing false positives and false negatives, and providing policy compliance and enforcement capabilities.

Market Requirements

The latest network compromises are combining qualities of viruses, worms, and direct compromise attacks into new blended attacks and may utilize metamorphic or polymorphic abilities to change their signatures to avoid detection.

To mitigate these new risks, organizations are now deploying a multi-tiered network defense strategy comprised of a variety of additional point products layered at the perimeter and to internal network machines and devices.

However, the point products rely on signatures or anomalies, producing an ever-increasing quantity of data, including false positive and false negatives. They also lack the intelligence to identify, reference, or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintained numerous point products is overwhelming the end user.

Therefore, a more sophisticated, intelligent technology is needed to resolve these issues.

Solution

SecurityProfiling now offers an intelligent integration platform and SDK — the first Anti-Vulnerability technology to meet market requirements.

Functional Description

1. **Integrates point products and provides system intelligence.** The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats.

2. **Cross-references the vulnerability targeted by the threat.** The vulnerability targeted by the threat is attained by the point products and the CVE ID or other identifier is fed into the logic engine where it is cross-referenced with the vulnerabilities of the targeted machine. An answer is returned accurately indicating if the machine is vulnerable.

3. **Identifies network vulnerabilities.** The platform will independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

SCP0052203
ForcePoint LLC
EX-1002
Page294

4. **Remediates the vulnerability.** Once a vulnerability is identified, a remediation functionality is provided that may automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

Functionalities Integrated with the SDK

Functionalities that may be integrated into point products with the SDK:

1. Group Management Functions
2. Client Management Functions
3. Update Management Functions
4. Polling Management Functions
5. Vulnerability Query Functions
6. Conversion Functions

Detailed descriptions are provided in Appendix I, and the SDK User's Guide.

SDK Applications - Example Product Integration

Examples of additional functionalities that may be integrated into point products via the SDK for enterprise and small office home office (SOHO) networks:

1. Patch Deployment – Remotely remediates network vulnerabilities and provides policy compliance and enforcement capabilities. See SecurityProfiling's SysUpdate white paper and trial download online.
2. IDS –Eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities.
3. Scanner - Eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities.
4. Firewall - Eliminates false positive and false negatives, preventing the security system from denying valid traffic to the organization - self-inflicted denial of service attacks, and adds vulnerability remediation, and policy compliance and enforcement functionalities.
5. Vulnerability Management – Same as 1., above.
6. Multiple Products: IDS, Scanner, and Firewall - Each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats.
7. Client Security - Attain the additional functionalities and benefits as the multiple products listed above, yet are even more effective since they additionally communicate and share information directly with each other. They will also attain vulnerability identification, reference, remediation, and policy compliance and enforcement capabilities.

SCP0052204
ForcePoint LLC
EX-1002
Page295

Components

The Anti-Vulnerability platform is comprised of the platform software components: SDK, Client Agent, Logic Engine, and Data Warehouse. Network Operations Center (NOC) Servers periodically synchronize the customer's servers with the latest vulnerability and update data. Please reference the Platform component Diagram on page x.

System Requirements

There are two system requirements: TCP/IP connectivity, and supported network machines and devices. Platforms supported are:

- All Windows Operating Systems and their applications
- All UNIX variants
- Cisco routers and firewalls
- Linksys network devices
- Netgear network devices
- Toshiba network devices

Platform support is scalable to any network size or architecture; consumer, small office home office (SOHO), enterprise, and distributed networks.

SCP0052205
ForcePoint LLC
EX-1002
Page296

What is the SDK and Anti-Vulnerability Platform ?

The SDK was designed to be a simple integration pathway to the back-end Anti-Vulnerability platform - consisting of a logic engine and vulnerability data warehouse. It will enable any network security product such as an IDS, scanner, or firewall to intelligently reference and share the same vulnerability data set, and provide complete vulnerability remediation functionalities. Thereby, improving system accuracy and efficiencies, minimizing false positives and false negatives, and providing policy compliance and enforcement capabilities.

A product architect simply chooses the functionality desired, inserts the provided functionality SDK sample code into the product code. (Detailed in a separate document, titled: *SDK User's Guide*.) The SDK sample code will then query –via the logic engine - the Anti-Vulnerability data warehouse, and in turn will return an answer to the point product. The architect can then show the results in any format desired in the product's interface. Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well.

Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience.

Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy - increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance functionality.

Insert Diagram 1 – SDK and Platform Overview Diagram

For more detail, see the Platform component Diagram on page x, and the Platform Query Functionality Diagram on page y.

SCP0052206
ForcePoint LLC
EX-1002
Page297

Market Requirements

Networks are probed at an ever-increasing frequency for vulnerabilities, which may be subsequently exploited with compromise attacks. To protect the network, administrators have traditionally set up perimeter defense strategies.

These strategies generally call for network managers to lock down core servers, and monitor/scan/filter all incoming and outgoing traffic at the network perimeter with several point products such as antivirus and firewalls to identify and attempt to neutralize hackers and malicious code. In the past, these strategies worked well, however new threats are becoming more complex.

The latest malicious code may combine qualities of viruses, worms, and direct compromise attacks into new *blended* attacks. Virus payloads are becoming more complex and by using metamorphic or polymorphic abilities, viruses are able to change their signatures to avoid the fingerprint-type filtering that most applications employ.

To mitigate these new risks, organizations are now deploying a multi-tiered network defense strategy comprised of a variety of additional point products layered at the perimeter and to internal network machines and devices. Such point products include anti-virus, firewall, scanners, and network and host Intrusion Detection Systems.

Each of these systems is based on specific signatures, rules, or anomalies of each malicious code and their variants, and do not identify and remediate the specific network vulnerabilities the code is targeting. So each code, and its variants, must be identified and analyzed, a signature prepared, then finally deployed to each point product on each customer's network. This process is uncoordinated among multiple disparate systems, creates an ever-increasing number of signatures producing more and more attack alerts requiring immediate attention – many of which are erroneous.

Additionally, to proactively remediate the vulnerabilities the malicious code is targeting, administrators must quickly and diligently update or "patch" each network machine and device, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives now require higher standards of network security and integrity to protect consumer privacy, and they must be documented with change tracking and audit trail reports.

Therefore, it is increasingly difficult and costly to effectively mitigate new threats and manage numerous systems - particularly in an environment of rising security standards and policy compliance requirements.

Thus, the multi-tiered network defense strategy is falling short primarily for four reasons:

1. The inability of multi-tiered point products to communicate and share information necessary to mitigate blended threats, and minimize false positives and false negatives.

2. The vulnerability targeted by malicious code is not accurately identified nor proactively remediated.

3. The associated excessive aggregate cost of ownership of multiple systems.

SCP0052207
ForcePoint LLC
EX-1002
Page298

4. The excessive administrative burden and cost of managing and maintaining multiple systems.

Hence, there is a need to integrate systems, share information intelligently to better defend against blended threats, reduce management and cost requirements, and automate vulnerability identification and remediation functionalities, as presented in the high-level requirements.

New Technology High-Level Requirements

A new technology is needed to meet market requirements:

1. Integrate point products to share information
2. Provide system intelligence.
3. Remediate network vulnerabilities.

SCP0052208
ForcePoint LLC
EX-1002
Page299

Solution

SecurityProfiling now offers an intelligent integration platform and SDK — the first Anti-Vulnerability technology to meet market requirements. The SDK and Anti-Vulnerability platform will enable product architects to integrate the ability for their products to intelligently reference and share information from the same vulnerability data set, provide vulnerability identification and remediation functionalities, and efficiently meet policy compliance and enforcement requirements.

The Anti-Vulnerability platform is a complimentary network security technology. When integrated into the defense strategy, it adds intelligence that more accurately and efficiently mitigates blended threats and offloads the time-consuming functions that burden network administrators.

The platform's enables point products to share information via its proprietary **logic engine** automatically cross-references the vulnerability the threat is targeting with the targeted machine or device to determine if it is vulnerable to that threat. Accuracy and efficiencies are realized, and the need to layer more and more point products is reduced. Subsequently, the costs to acquire, operate, and manage the additional multiple point products are also reduced.

The platform will also remotely remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented.

Insert Diagram 2 – SDK and Platform Component Diagram

Features & Benefits

Features:

The Anti-Vulnerability™ platform and SDK fulfills market requirements noted in the previous section.

1. **Integrates point products and provides system intelligence.** The same vulnerability data warehouse information is shared to the products so that more intelligent actions may then be taken to mitigate complex threats.

2. **Cross-references the vulnerability targeted by the threat.** The vulnerability targeted by the threat is attained by the point products and the CVE ID or other identifier is fed into the logic engine where it is cross-referenced with the vulnerabilities of the targeted machine. An answer is returned indicating if the machine is vulnerable.

3. **Identifies network vulnerabilities.** The platform will independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

4. **Remediates the vulnerability.** Once a vulnerability is identified, a remediation functionality is provided that may automatically deploy the

SCP0052209
ForcePoint LLC
EX-1002
Page300
C

appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

These functionalities will be presented in more detail in the next section ---- Functional Description.

Benefits:

Blended attacks are more effectively mitigated and the overwhelming management and maintenance burden on administrators to purchase, operate, and maintain multiple point products is reduced, while increasing productivity, reducing costs, and more effectively and efficiently meeting policy compliance and enforcement requirements.

Benefits to technology providers and end users:

Security Companies

- Supplements existing technology to better defend against blended attacks

  Intelligently accesses the vulnerability data warehouse, and remediates vulnerabilities

- Supports both the enterprise and SOHO networks

  Data warehouse contains vulnerabilities and updates for many machines and devices that operate on both enterprise and SOHO networks. See the Supported Platforms subsection for more details

- Minimize development time - speed to market

  SDK functionalities may be integrated with sample code provided in the SDK User's Guide

- Minimize end user education/ absorption costs

  The Anti-Vulnerability platform functionalities are transparently integrated, retaining pre-existing architecture, processes, and interfaces. Therefore, the end user experience remains the same, or improved with simplified or automated processes.

- Offers policy compliance and enforcement functionality

  Vulnerabilities may be automatically remediated, verified and documented, therefore enforcing compliance.

Product Architects

- Quick and easy integration process

  Simply insert the SDK sample code into the product code as detailed in the SDK User's Guide

- The SDK adds functionality to products transparently -- retaining pre-existing architecture and end user interfaces.

SCP0052210
ForcePoint LLC
EX-1002
Page301

The SDK integrates functionalities that return answers to the functional queries to the logic engine and data warehouse. The responses then may be incorporated into existing product user interfaces at the discretion of the architect.

End Users

- No additional software or hardware implementation costs

  Anti-Vulnerability functionalities may be integrated into existing product platforms

- Reduces cost of ownership of multi point products

  Shared vulnerability data sets and added vulnerability remediation functionalities may reduce the number of point products needed to adequately attain defense strategy requirements.

- Reduces point product management and maintenance costs

  Increased accuracy of vulnerability identification, remediation and policy enforcement, and reduction of false positive, false negatives and denial of service (DoS), significantly reduces management time and costs.

- Manage more machines and devices on the network through one portal

  Vulnerability remediation and policy compliance and enforcement may be integrated with existing security point products, and their respective interfaces.

- User experience remains the same – additional time or costs to understand and execute new technologies are minimized.

  Anti-Vulnerability functionalities may be integrated transparently and seamlessly, and the pre-existing processes and interfaces are virtually unaffected.

SCP0052211
ForcePoint LLC
EX-1002
Page302

Functional Description

This section provides the functionality query flow chart, and the functionalities, by group, that may be integrated into point products with the SDK.

The functionalities access the platform with queries to generate the desired answers. Below is how the queries flow through the platform.

Insert Diagram 3 – Functionality Query Flow Chart

An overview of the functions that may be integrated via the SDK is provided below. The functions are presented in groups, and a full listing with parameters and returned answer format is presented in Appendix I. More detail, and step-by-step integration procedures are presented in the SDK User's Guide.

Functionality Groups:

1. **Group Management Functions**
2. **Client Management Functions**
3. **Hot Fix Management Functions**
4. **Polling Functions**
5. **Vulnerability Query Functions**
6. **Conversion Functions**

1. Group Management Functions

a. **CreateGroup** – This function creates a new group.

b. **GetGroups** –This function returns a list of all configured groups.

c. **DeleteGroup** –This function removes a group.

d. **GetGroupPolicy** –This function returns the policy for a group

e. **SetGroupPolicy** –This functions sets a new policy for a group

SCP0052212
ForcePoint LLC
EX-1002
Page303
C

f. GetClientsInGroup –This function retrieves a list of clients that are members of a specific group

g. AddClientToGroup –This function adds a client to a group

h. RemoveClientFromGroup –This function removes a client from a group.

2. Client Management Functions

a. GetClientHardwareStats - This function retrieves information about the client's hardware configuration

b. GetClientInstalledSoftware -This function retrieves information about software installed on the client.

c. GetClientInstalledHotfixes –This function retrieves a list of hot fixes that were verified as installed on the last polling

d. GetClientPendingUpdates This function returns a list of hot fixes that the client needs (according to group policy) as of the last polling.

e. GetClientLogs - This function returns a list of log entries for a particular client.

f. ResetClient –This function causes the client to reset, thus forcing it to regenerate all information about its state.

g. DeleteClient –This function removes all information pertaining to this client from the SysUpdate database.

h. GetClientHotFixStatus –This function retrieves information about a particular hot fix on a machine, such as: is it needed, is it installed, is it pending, is it send, etc.

3. Update Management Functions

a. GetHotFixInfo –This function retrieves detailed information about a particular update.

b. InstallHotFixForClient –This function installs an update on a particular client if applicable.

c. InstallHotFixForGroup –This function installs an update on all clients in a group that need it.

d. InstallAllPendingClient –This function installs all pending update on a client.

e. InstallAllPendingGroup –This function installs all pending updates on all clients in a group.

f. RejectHotFixForClient – This function rejects an update for a particular client.

SCP0052213
ForcePoint LLC
EX-1002
Page304

g. **RejectHotFixForGroup** –This function rejects an update on all clients in a particular group.

h. **RequeueHotFixForClient** –This function cancels a previous update rejection for a particular client.

i. **RequeueHotFixForGroup** - This function cancels a previous update rejection for all clients in a particular group.

j. **RemoveHotFixFromClient** –This function removes a previously installed update

k. **RemoveHotFixFromGroup** –This function removes an update on all clients in a group that have that hot fix installed.

4. Polling Functions

a. **PollClient** –This function causes a client to be polled by the onsite server immediately.

b. **PollGroup** –This function causes all the clients in a particular group to be polled immediately.

c. **PollAll** –This function causes all clients to be polled immediately.

d. **IsPolling** –This function returns TRUE if the OnSite Server is in the process of polling clients.

5. Vulnerability Query Functions

a. **QueryVulnerabilityByCveID** –This function retrieves whether or not the client is vulnerable to a particular CVE id.

b. **QueryVulnerabilityByQID** - This function retrieves whether or not the client is vulnerable to a particular Q id.

c. **QueryVulnerabilityByMSID** –This function retrieves whether or not the client is vulnerable to a particular MS id.

d. **QueryVulnerabilityByBugtraqID** –This function retrieves whether or not the client is vulnerable to a particular Bugtraq id.

6. Conversion Functions

a. **CveID2QID** –This function converts a CVE id to a corresponding Q id.

b. **CveID2MSID** – This function converts a CVE id to a corresponding MS id.

c. **CveID2BugtraqID** – This function converts a CVE id to a corresponding Bugtraq id.

SCP0052214
ForcePoint LLC
EX-1002
Page305

d. **QID2CveID** – This function converts a Q id to a corresponding CVE id.

e. **QID2MSID** – This function converts a Q id to a corresponding MS id.

f. **QID2BugtraqID** – This function converts a Q id to a corresponding Bugtraq id.

g. **MSID2CveID** – This function converts an MS id to a corresponding CVE id.

h. **MSID2QID** –This function converts an MS id to a corresponding Q id.

i. **MSID2BugtraqID** – This function converts an MS id to a corresponding Bugtraq id.

j. **BugtraqID2CveID** –This function converts a Bugtraq id to a corresponding CVE id.

k. **BugtraqID2QID** – This function converts a Bugtraq id to a corresponding Q id.

l. **BugtraqID2MSID** –This function converts a Bugtraq id to a corresponding MS id.

SCP0052215
ForcePoint LLC
EX-1002
Page306

SDK Applications - Example Product Integration

This section provides examples of SDK applications, and their benefits, when the functionalities from the previous section are integrated into specific or multiple products.

1. Patch Deployment

SecurityProfiling's SysUpdate vulnerability remediation solution has incorporated virtually all of the functionalities listed in the previous section. A white paper and trial download is available online that demonstrate its functionalities and benefits.

Benefits:

The SDK and platform enables products to add accurate vulnerability identification, remediation, verification, and policy compliance.

With the SDK, the product will gain intelligence, accuracy and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks.

2. IDS

IDS products attempt to identify malicious code by signatures at both the network and host client level based. While they may be able to identify its CVE ID or other vulnerability identifier, and target, they generally do not have the intelligence to determine if the any of the machines on the network are susceptible to that attack, or with finer granularity, if any machine has a specific vulnerability to that specific attack.

For example, if the attack is a Window based attack targeting a Windows machine. Is the targeted machine actually running Windows, and if so, is the machine vulnerable to the attack? Lastly, if so, the targeted vulnerability remains unremediated – the IDS system can not remediate it.

Benefits:

With the SDK, a product architect can integrate functionalities listed in the previous secti on to enable the IDS to access the anti-vulnerability logic engine and platform. It will then have the intelligence to determine if any machine on the network is susceptible to the attack, remediate the vulnerability, mitigate the attack, and verify policy compliance.

Now, if no machines were susceptible to the attack, the code is identified as a false positive, no further data or alert is generated, and a management response is not required.

With the SDK and platform, the product will gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks.

SCP0052216
ForcePoint LLC
EX-1002
Page307
C

3. Scanners

Vulnerability scanners assess each machine on the network for vulnerabilities, and create lists of potential vulnerabilities to the system managers. The lists commonly contain many false positives and false negatives, burdening the system and managers with inaccuracies.

Benefits

With the SDK, a product architect can integrate functionalities listed in the previous section to enable the scanner to access the anti-vulnerability logic engine and platform, and then have the intelligence to determine if the machine has actual vulnerabilities, remediate them, and verify policy compliance.

With the SDK and platform, the product will gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money.

4. Firewall

"Smart" firewalls are based in part on signatures and other similar functionalities as IDS products described above.

With the SDK and platform the firewall can determine whether an attack is valid or a false positive, thereby preventing the security system from denying valid traffic to the organization - self-inflicted DoS attacks.

Such functionalities and benefits are available for both the enterprise and SOHO networks.

5. Vulnerability Management

Vulnerability Management products enable managers to set policy and identify potential network vulnerabilities. They typically do not accurately identify each vulnerability on each network machine and device, nor remediate each vulnerability, meeting policy compliance enforcement requirements.

Benefits:

The SDK and platform offer similar functionalities and benefits as the patch deployment products described above. In short, it enables products to add accurate vulnerability identification, remediation, verification, and policy compliance.

Such functionalities and benefits are available for both the enterprise and SOHO networks.

6. Multiple Products: IDS, Scanner, and Firewall

Each product functions as the individual products noted above. Each may be deployed and operate on the network in a multi-tiered network defense strategy. They may be disparate system, and their signatures and update deployment schedules may vary. Therefore, the probability of mitigating a new and complex threat decreases, while management requirements and cost increases.

Benefits:

With the SDK and platform, they each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats.

SCP0052217
ForcePoint LLC
EX-1002
Page308

7. Client Security

Client security products offer an integrated antivirus, firewall, and IDS functionality.

With the SDK and platform, they attain the additional functionalities and benefits as the multiple products listed above, yet are even more effective since they additionally communicate and share information directly with each other. They will also attain vulnerability identification, reference, remediation, and policy compliance and enforcement capabilities.

Such functionalities and benefits are available for both the enterprise and SOHO networks.

SCP0052218
ForcePoint LLC
EX-1002
Page309

Technical Description

This section consists of a detailed description of the platform's components, the NOC Servers, and system requirements:

Client Agent

Logic Engine

Data Warehouse

Network Operations Center (NOC) Servers

System Requirements

Client Agent

The agent is remotely deployed to each machine or device on the network, and has two primary functions.

1. Accurately identifies the OS, applications, firmware, and updates installed on each machine or device.

2. Installs the updates.

Identifies Applications Installed

The client agent accurately identifies and inventories the operating system, applications, and updates installed on each machine. Periodically, the on-site server polls each client agent and the configuration data is transferred back to the server. The logic engine determines and deploys the appropriate updates to each machine. (More detail of this process is provided in the next sub-section, -- Logic Engine.)

Installs the Updates

There, the client agent installs the updates, and verifies they are running correctly.

This cycle is repeated each polling interval. Should an update not be installed properly, or even if the user (or intruder) accidentally or purposely deletes an update, the system will re-install it.

SCP0052219
ForcePoint LLC
EX-1002
Page310

Client Agent Component	Application size:	The client agent is about 1 MB, and is virtually undetectable.
	Application Type:	Automatic Service
	Connectivity Required:	TCP/IP
	Compatibility/Stability:	In lab testing, the agent has been shown to be compatible with other agents, such as anti-virus agents. To date, customers have not encountered any problems.
	User Options:	Run queued updates, only.
	Security:	Updates sent to each client in an AES-encrypted format.

Logic Engine

The logic engine, or system intelligence, cross references the vulnerability the threat is targeting and the targeted machine or device vulnerabilities through the data warehouse, and returns the answer to the point product.

It also determines which updates are needed and compatible with each machine's configuration.

The logic engine cross-references and matches each client's configuration with the information for each update, and determines which updates are appropriate. It then takes these results and filters them through the group policy to determine which updates should actually be installed on the client. Lastly the logic engine once more references the group policy to determine what action (if any) to take, and then performs this action at the appropriate time.

SCP0052220
ForcePoint LLC
EX-1002
Page311

Data Warehouse

This component has five primary functions:

1. For vulnerability remediation functionalities, periodically polls the clients for configuration data.
2. Maintains the vulnerability database.
3. Maintains the update database.
4. Periodically polls the NOC server, and receives updates.

Client Agent Polling

The client agents are periodically polled for client configuration dataa. Each client responds with their respective OS, applications, firmware and updates installed, which will be cross-refcrenced by the logic engine.

Vulnerability Database

The data warehouse fully maintains a full vulnerability database. The database is a self-configuring, self-populating, maintenance-free database, and does not require administrator inputs or interaction. The database periodically synchronizes itself with the NOC servers' database.

The database was designed to accommodate and organize all vulnerabilities across the network with a proprietary schema. The schema was also designed to be accessible to unique queries to cross-reference its data. The logic engine determines which fields are to be queried, and returns the processed data results.

Update Database

The on-site server component fully maintains an update database. The database is a self-configuring, self-populating, maintenance-free database, and does not require administrator inputs or interaction. The database periodically synchronizes itself with the NOC servers' database, as noted below.

NOC Server Polling

The NOC servers are polled on an hourly basis, and operate on a "pull" traffic network. The only information leaving the customer's site is an encrypted key, used for authentication by the NOC servers. Once authenticated, the servers are synchronizes with the latest vulnerabilities and updates. These files are sent in an AES-encrypted format.

SCP0052221
ForcePoint LLC
EX-1002
Page312

Server Component	Space required:	The server component requires 40 GB of space.
	Security:	Updates pulled from NOC Servers are in an AES-encrypted format.
	Polling Interval:	The on-site server polls the clients at any interval selected by the administrator.

Network Operations Center (NOC) Servers

The vulnerabilities and updates and their respective guidelines are archived in the Anti-Vulnerability™ NOC servers' database and periodically distributed to the customer's site.

System Requirements

There are two system requirements: TCP/IP connectivity, and network platforms supported.

The application is scalable to any network size or architecture, and only requires TCP/IP connectivity between the client and the server.

The platform is compatible with any machines or device:

- Windows
- All UNIX variants
- Cisco routers and firewalls
- Linksys network devices
- Netgear network devices
- Toshiba network devices

SCP0052222
ForcePoint LLC
EX-1002
Page313

Conclusion

The Anti-Vulnerability platform and SDK is an intelligent technology that will supplement any existing defense strategy. It integrates point products so they may share the same vulnerability data set to improve automation and accuracy - increasing efficiencies and minimizing false positives and false negatives. It also enables remote identification, management, and remediation of network vulnerabilities, and provides update deployment, validation, and reporting capabilities. Thereby, the platform and SDK improves network security and integrity, better mitigating blended threats, while increasing productivity, saving time and money, and more effectively and efficiently attaining policy compliance and enforcement requirements.

Appendix I – Integration Functionalities, by Group

Anti-Vulnerability functions that are accessible via the SDK. The functions are presented in groups, as follows:

Group Management Functions
Client Management Functions
Hot Fix Management Functions
Polling Functions
Vulnerability Query Functions
Conversion Functions

Group Management Functions

- **CreateGroup** – Parameters: GROUP structure defining the new group
  Returns: Success or failure.
  Description: This function creates a new group.
- **GetGroups** – Parameters: None
  Returns: An array of GROUP structures.
  Description: This function returns a list of all configured groups.
- **DeleteGroup** – Parameters: GROUP structure to be deleted.
  Returns: Success or failure
  Description: This function removes a group.
- **GetGroupPolicy** – Parameters: GROUP structure to get the corresponding POLICY structure from.
  Returns: POLICY structure corresponding to the passed GROUP
  Description: This function returns the policy for a group
- **SetGroupPolicy** – Parameters: GROUP structure to receive new policy, POLICY structure to set for the group
  Returns: Success or failure
  Description: This functions sets a new policy for a group
- **GetClientsInGroup** – Parameters: GROUP structure to retrieve the clients from
  Returns: Array of CLIENT structures belonging to the group
  Description: This function retrieves a list of clients that are members of a specific group
- **AddClientToGroup** – Parameters: CLIENT structure to add to a group, GROUP structure to add the client to.
  Returns: Success or failure
  Description: This function adds a client to a group
- **RemoveClientFromGroup** – Parameters: CLIENT structure to remove from group, GROUP structure to remove the client from
  Returns: Success or failure.
  Description: This function removes a client from a group.

Client Management Functions

- **GetClientHardwareStats** – Parameters: CLIENT structure to get information from.

SCP0052224
ForcePoint LLC
EX-1002
Page315

Returns: CLIENT_HARDWARE structure describing the client's hardware configuration

Description: This function retrieves information about the client's hardware configuration

- **GetClientInstalledSoftware** – Parameters: CLIENT structure to get information from.
  Returns: CLIENT_SOFTWARE structure describing software install on the client.

Description: This function retrieves information about software installed on the client.

- **GetClientInstalledHotfixes** – Parameters: CLIENT structure to get information from.
  Returns: Array of HOTFIX structures corresponding to the installed hot fixes on the client

Description: This function retrieves a list of hot fixes that were verified as installed on the last polling

- **GetClientPendingUpdates** – Parameters: CLIENT structure to get information from.
  Returns: Array of HOTFIX structures corresponding to the pending hot fixes for the client

Description: This function returns a list of hot fixes that the client needs (according to group policy) as of the last polling.

- **GetClientLogs** - Parameters: CLIENT structure to get information from
  Returns: Array of CLIENT_LOG structures containing log entries for the client.

Description: This function returns a list of log entries for a particular client.

- **ResetClient** – Parameters: CLIENT structure to reset.
  Returns: Success or failure.

Description: This function causes the client to reset, thus forcing it to regenerate all information about its state.

- **DeleteClient** – Parameters: CLIENT structure to delete.
  Returns: Success or failure.

Description: This function removes all information pertaining to this client from the SysUpdate database.

- **GetClientHotFixStatus** – Parameters: CLIENT structure to get information from, HOTFIX structure to get information about
  Returns: Code to indicate the status of the hot fix with respect to that client, or failure.

Description: This function retrieves information about a particular hot fix on a machine, such as: is it needed, is it installed, is it pending, is it send, etc.

Update Management Functions

- **GetHotFixInfo** – Parameters: HOTFIX structure to get information from
  Returns: HOTFIX_INFO structure describing the update
  Description: This function retrieves detailed information about a particular update.
- **InstallHotFixForClient** – Parameters: HOTFIX structure to install, CLIENT structure to install the update on.
  Returns: Success or failure.

  Description: This function installs an update on a particular client if applicable.

- **InstallHotFixForGroup** – Parameters: HOTFIX structure to install, GROUP structure to deploy the update to.

SCP0052225
ForcePoint LLC
EX-1002
Page316

Returns: Success or failure.

Description: This function installs an update on all clients in a group that need it.

- **InstallAllPendingClient** – Parameters: CLIENT structure to install update on
  Returns: Success or failure.

  Description: This function installs all pending updates on a client.
- **InstallAllPendingGroup** – Parameters: GROUP to deploy update to.
  Returns: Success or failure.

  Description: This function installs all pending updates on all clients in a group.
- **RejectHotFixForClient** – Parameters: HOTFIX structure to reject, CLIENT structure to reject update on.
  Returns: Success or failure.

  Description: This function rejects an update for a particular client.
- **RejectHotFixForGroup** – Parameters: HOTFIX structure to reject, GROUP structure to reject update for.
  Returns: Success or failure.

  Description: This function rejects an update on all clients in a particular group.
- **RequeueHotFixForClient** – Parameters: HOTFIX structure to requeue, CLIENT structure to requeue the update on.
  Returns: Success or failure.

  Description: This function cancels a previous update rejection for a particular client.
- **RequeueHotFixForGroup** – Parameters: HOTFIX structure to requeue, GROUP structure to requeue the update for.
  Returns: Success or failure.

  Description: This function cancels a previous update rejection for all clients in a particular group.
- **RemoveHotFixFromClient** – Parameters: HOTFIX structure to remove, CLIENT structure to remove the update from.
  Returns: Success or failure.

  Description: This function removes a previously installed update

SCP0052226
ForcePoint LLC
EX-1002
Page317

- **RemoveHotFixFromGroup** – Parameters: HOTFIX structure to remove, GROUP structure to remove the update from
  Returns: Success or failure.

  Description: This function removes an update on all clients in a group that have that hot fix installed.

Polling Functions

- **PollClient** – Parameters: CLIENT structure to poll
  Returns: Success or failure.
  Description: This function causes a client to be polled by the onsite server immediately.
- **PollGroup** – Parameters: GROUP structure to poll
  Returns: Success or failure.

  Description: This function causes all the clients in a particular group to be polled immediately.

- **PollAll** – Parameters: NONE
  Returns: Success or failure.

  Description: This function causes all clients to be polled immediately.
- **IsPolling** – Parameters: NONE
  Returns: TRUE or FALSE
  Description: This function returns TRUE if the OnSite Server is in the process of polling clients.

Vulnerability Query Functions

- **QueryVulnerabilityByCveID** – Parameters: CLIENT structure to get information from, CVEID structure to get information about
  Returns: Code indicating status of machine with respect to the CVE id
  Description: This function retrieves whether or not the client is vulnerable to a particular CVE id.
- **QueryVulnerabilityByQID** – Parameters: CLIENT structure to get information from, QID structure to get information about.
  Returns: Code indicating status of machine with respect to the Q id
  Description: This function retrieves whether or not the client is vulnerable to a particular Q id.
- **QueryVulnerabilityByMSID** – Parameters: CLIENT structure to get information from, MSID structure to get information about.
  Returns: Code indicating status of machine with respect to the MS id
  Description: This function retrieves whether or not the client is vulnerable to a particular MS id.

- **QueryVulnerabilityByBugtraqID** – Parameters: CLIENT structure to get information from, BUGTRAQID structure to get information about.
  Returns: Code indicating status of machine with respect to the Bugtraq id
  Description: This function retrieves whether or not the client is vulnerable to a particular Bugtraq id.

Conversion Functions

SCP0052227
ForcePoint LLC
EX-1002
Page318

- **CveID2QID** – Parameters: CVEID Structure to convert
  Returns: QID Structure corresponding to a CVE id
  Description: This function converts a CVE id to a corresponding Q id.
- **CveID2MSID** – Parameters: CVEID Structure to convert
  Returns: MSID Structure corresponding to a CVE id
  Description: This function converts a CVE id to a corresponding MS id.

- **CveID2BugtraqID** – Parameters: CVEID Structure to convert
  Returns: BUGTRAQID Structure corresponding to a CVE id
  Description: This function converts a CVE id to a corresponding Bugtraq id.

- **QID2CveID** – Parameters: QID Structure to convert
  Returns: CVEID Structure corresponding to a Q id
  Description: This function converts a Q id to a corresponding CVE id.

- **QID2MSID** – Parameters: QID Structure to convert
  Returns: MSID Structure corresponding to a Q id
  Description: This function converts a Q id to a corresponding MS id.
- **QID2BugtraqID** – Parameters: QID Structure to convert
  Returns: BUGTRAQID Structure corresponding to a Q id
  Description: This function converts a Q id to a corresponding Bugtraq id.
- **MSID2CveID** – Parameters: MSID Structure to convert
  Returns: CVEID Structure corresponding to an MS id
  Description: This function converts an MS id to a corresponding CVE id.
- **MSID2QID** – Parameters: MSID Structure to convert
  Returns: QID Structure corresponding to an MS id
  Description: This function converts an MS id to a corresponding Q id.
- **MSID2BugtraqID** – Parameters: MSID Structure to convert
  Returns: BUGTRAQID Structure corresponding to an MS id
  Description: This function converts an MS id to a corresponding Bugtraq id.
- **BugtraqID2CveID** – Parameters: BUGTRAQID Structure to convert
  Returns: CVEID Structure corresponding to a Bugtraq id
  Description: This function converts a Bugtraq id to a corresponding CVE id.
- **BugtraqID2QID** – Parameters: BUGTRAQID Structure to convert
  Returns: QID Structure corresponding to a Bugtraq id
  Description: This function converts a Bugtraq id to a corresponding Q id.
- **BugtraqID2MSID** – Parameters: BUGTRAQID Structure to convert
  Returns: MSID Structure corresponding to a Bugtraq id
  Description: This function converts a Bugtraq id to a corresponding MS id.

Financial benefits were core considerations in the design and implementation of SysUpdate™. The goal is to maximize value and minimize cost.

The cost of manually updating each server and workstation with existing technologies is indeed prohibitive, as demonstrated by the process and associated costs shown in Figure 14, below.

SCP0052228
ForcePoint LLC
EX-1002
Page319

Appendix V – About SecurityProfiling

About SecurityProfiling

Founded in 1998, *SecurityProfiling* has developed into a nationally recognized leader in network computer security and software application development. Initially specializing in risk assessments, network architecture development, and forensic work, *SecurityProfiling* has evolved into the world-class network software innovator it is today. Realizing the need for a truly effective and automated software update management application, *SecurityProfiling* has developed and implemented SysUpdate™, a nationally recognized product — the first Anti-Vulnerability™ technology.

Utilizing the revolutionary automation processes that was developed for SysUpdate™, *SecurityProfiling* then developed LogBoss™, a comprehensive network log manager that allows administrators to manage, archive, query, and report all network logs.

Below is a list of *SecurityProfiling's* products and services.

Risk Assessment: A comprehensive security audit of an organization's network infrastructure, followed by a detailed prioritized report of all vulnerabilities that also includes understandable recommendations to solve these issues.

SysUpdate™: A new and revolutionary product that not only provides any organization a higher level of security, but also saves time for administrators. This product automatically installs and upgrades "hotfixes", security patches, and service packs, while also providing excellent centralized reporting and auditing capabilities.

LogBoss™: A secure, easy to use network log manager offering fully automated archiving, cross-querying, and reporting for all network logs, (security, application, & system)… no matter how large or how complex the network. With LogBoss™, administrators will now know what has happened on their network, regardless of the type of event or when it occurred. LogBoss™ also helps comply with HIPAA, GLBA, and ISO 9001 standards.

Emergency Response Expertise: In the unfortunate event of a security compromise, *SecurityProfiling* can assist in recovery and evidence procurement, minimizing company downtime and expense.

IDS (Intrusion Detection System): Provides a "port hole" view to the security of an organization's infrastructure. With IDS, policy & reporting actions are essential to the effectiveness of the system. *SecurityProfiling* fills this gap by consulting with key security personnel to implement 'Policy to Procedure' actions for the IDS infrastructure.

Computer Forensics: *SecurityProfiling's* excellent reputation is often called upon to assist both law enforcement and private industry to determine exactly the problems encountered, retrieve data, identify culprits, and provide expert witness testimony.

Wireless Security Consulting: Wireless technology is inherently vulnerable to compromise. With assistance from SecurityProfiling, an organization can receive the benefits of wireless technology without sacrificing security.

SCP0052229
ForcePoint LLC
EX-1002
Page320

Staff Security Training: Computer security training is the only long-term solution to truly protect any organization. Training personnel on relevant security issues raises awareness, prevents security mistakes, and empowers the organization, and such policy is a requirement mandated by HIPAA and GLBA.

For further information regarding SecurityProfiling's products and services, please contact us at:



SECURITYPROFILING

839 Main St.
Suite 405
Lafayette, IN 47901
Toll Free: (888) 645-3676
Phone: (765) 420-7227
Fax: (765) 420-9256
E-Mail: info@securityprofiling.com

www.securityprofiling.com

SCP0052230
ForcePoint LLC
EX-1002
Page321

Field	Content
PRODBEG	SCP0052200
PRODEND	SCP0052230
PRODBEGATT	SCP0052200
PRODENDATT	SCP0052230
ATTRANGE	SCP0052200-SCP0052230
ATTACHCOUNT	
ATTACHMENTS	
PRODVOLUME	
REVIEWBEGDOC	
CUSTODIAN	
ALLCUSTODIAN	
AUTHOR	John Blignaut
FROM	
TO	
CC	
BCC	
SORTDATE	00/00/0000
SORTTIME	
SENTDATE	00/00/0000
SENTTIME	
RECEIVEDDATE	00/00/0000
RECEIVEDTIME	
MODDATE	09/27/2002
MODTIME	07:46 PM
DATECREATED	09/26/2002
TIMECREATED	12:03 PM
PAGECOUNT	
SUBJECT	
DOCTYPE	
FILETYPE	
DOCTITLE	Contemporary Report
MD5HASH	D7EB44DE5BBA557C3010445F68477074
GROUPMD5HASH	
FILENAME	SDK Paper v1.0 9.27.02.doc
FILESIZE	223744
FILEEXT	doc
ORIGFOLDER	
ORIGLOCATION	Discovery - SP Doc Production\SDK - Not Confidential\SDK Pap...
CONVID	
IMPORTANCE	

ANNEX B

Application No.: 15/608,978	**Excerpts from Annex A**
21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;	See excerpt(s) below and/or other related disclosures in Annex A: *About SecurityProfiling* Founded in 1998, *SecurityProfiling* has developed into a nationally recognized leader in network computer security and software application development. Initially specializing in risk assessments, network architecture development, and forensic work, *SecurityProfiling* has evolved into the world-class network software innovator it is today. Realizing the need for a truly effective and automated software update management application, *SecurityProfiling* has developed and implemented SysUpdate™, a nationally recognized product — the first Anti-Vulnerability™ technology. Utilizing the revolutionary automation processes that was developed for SysUpdate™, *SecurityProfiling* then developed LogBoss™, a comprehensive network log manager that allows administrators to manage, archive, query, and report all network logs. Below is a list of *SecurityProfiling's* products and services. ***Risk Assessment:*** A comprehensive security audit of an organization's network infrastructure, followed by a detailed prioritized report of all vulnerabilities that also includes understandable recommendations to solve those issues. ***SysUpdate™:*** A new and revolutionary product that not only provides any organization a higher level of security, but also saves time for administrators. This product automatically installs and upgrades "hotfixes", security patches, and service packs, while also providing excellent centralized reporting and auditing capabilities. ***LogBoss™:*** A secure, easy to use network log manager offering fully automated archiving, cross-querying, and reporting for all network logs, (security, application, & system)… no matter how large or how complex the network. With LogBoss™, administrators will now know what has happened on their network, regardless of the type of event or when it occurred. LogBoss™ also helps comply with HIPAA, GLBA, and ISO 9001 standards. ***Emergency Response Expertise:*** In the unfortunate event of a security compromise, *SecurityProfiling* can assist in recovery and evidence procurement, minimizing company downtime and expense. ***IDS (Intrusion Detection System):*** Provides a "port hole" view to the security of an organization's infrastructure. With IDS, policy & reporting actions are essential to the effectiveness of the system. *SecurityProfiling* fills this gap by consulting with key security personnel to implement 'Policy to Procedure' actions for the IDS infrastructure. ***Computer Forensics:*** *SecurityProfiling's* excellent reputation is often called upon to assist both law enforcement and private industry to determine exactly the problems encountered, retrieve data, identify culprits, and provide expert witness testimony. ***Wireless Security Consulting:*** Wireless technology is inherently vulnerable to compromise. With assistance from SecurityProfiling, an organization can receive the benefits of wireless technology without sacrificing security. Page 29 of Annex A.

ForcePoint LLC
EX-1002
Page323

Components
The Anti-Vulnerability platform is comprised of the platform software components: SDK, Client Agent, Logic Engine, and Data Warehouse. Network Operations Center (NOC) Servers periodically synchronize the customer's servers with the latest vulnerability and update data. Please reference the Platform component Diagram on page x.

Page 5 of Annex A.

Data Warehouse
This component has five primary functions:

1. For vulnerability remediation functionalities, periodically polls the clients for configuration data.
2. Maintains the vulnerability database.
3. Maintains the update database.
4. Periodically polls the NOC server, and receives updates.

Client Agent Polling
The client agents are periodically polled for client configuration data. Each client responds with their respective OS, applications, firmware and updates installed, which will be cross-referenced by the logic engine.

Vulnerability Database
The data warehouse fully maintains a full vulnerability database. The database is a self-configuring, self-populating, maintenance-free database, and does not require administrator inputs or interaction. The database periodically synchronizes itself with the NOC servers' database.

The database was designed to accommodate and organize all vulnerabilities across the network with a proprietary schema. The schema was also designed to be accessible to unique queries to cross-reference its data. The logic engine determines which fields are to be queried, and returns the processed data results.

Update Database
The on-site server component fully maintains an update database. The database is a self-configuring, self-populating, maintenance-free database, and does not require administrator inputs or interaction. The database periodically synchronizes itself with the NOC servers' database, as noted below.

NOC Server Polling
The NOC servers are polled on an hourly basis, and operate on a "pull" traffic network. The only information leaving the customer's site is an encrypted key, used for authentication by the NOC servers. Once authenticated, the servers are synchronized with the latest vulnerabilities and updates. These files are sent in an AES-encrypted format.

Page 21 of Annex A.

Network Operations Center (NOC) Servers
The vulnerabilities and updates and their respective guidelines are archived in the Anti-Vulnerability™ NOC servers' database and periodically distributed to the customer's site.

Page 22 of Annex A.

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential	**Functional Description** 1. **Integrates point products and provides system intelligence.** The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats. 2. **Cross-references the vulnerability targeted by the threat.** The vulnerability targeted by the threat is attained by the point products and the CVE ID or other identifier is fed into the logic engine where it is cross-referenced with the vulnerabilities of the targeted machine. An answer is returned accurately indicating if the machine is vulnerable. 3. **Identifies network vulnerabilities.** The platform will independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly. Page 3 of Annex A. The platform's enables point products to share information via its proprietary **logic engine** automatically cross-references the vulnerability the threat is targeting with the targeted machine or device to determine if it is vulnerable to that threat. Accuracy and efficiencies are realized, and the need to layer more and more point products is reduced. Subsequently, the costs to acquire, operate, and manage the additional multiple point products are also reduced. The platform will also remotely remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented. Page 9 of Annex A. For example, if the attack is a Window based attack targeting a Windows machine. Is the targeted machine actually running Windows, and if so, is the machine vulnerable to the attack? Lastly, if so, the targeted vulnerability remains unremediated – the IDS system can not remediate it. Page 16 of Annex A.

vulnerabilities;	**Client Agent** The agent is remotely deployed to each machine or device on the network, and has two primary functions. 1. Accurately identifies the OS, applications, firmware, and updates installed on each machine or device. 2. Installs the updates. ***Identifies Applications Installed*** The client agent accurately identifies and inventories the operating system, applications, and updates installed on each machine. Periodically, the on-site server polls each client agent and the configuration data is transferred back to the server. The logic engine determines and deploys the appropriate updates to each machine. (More detail of this process is provided in the next sub-section, – Logic Engine.) Page 19 of Annex A. ***Logic Engine*** The logic engine, or system intelligence, cross references the vulnerability the threat is targeting and the targeted machine or device vulnerabilities through the data warehouse, and returns the answer to the point product. It also determines which updates are needed and compatible with each machine's configuration. The logic engine cross-references and matches each client's configuration with the information for each update, and determines which updates are appropriate. It then takes these results and filters them through the group policy to determine which updates should actually be installed on the client. Lastly the logic engine once more references the group policy to determine what action (if any) to take, and then performs this action at the appropriate time. Page 21 of Annex A.
identify an occurrence in connection with at least one of the plurality of devices; determine that the at least one accurately identified vulnerability	**Functional Description** 1. **Integrates point products and provides system intelligence.** The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats. 2. **Cross-references the vulnerability targeted by the threat.** The vulnerability targeted by the threat is attained by the point products and the CVE ID or other identifier is fed into the logic engine where it is cross-referenced with the vulnerabilities of the targeted machine. An answer is returned accurately indicating if the machine is vulnerable. Page 3 of Annex A.

of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and	The platform's enables point products to share information via its proprietary **logic engine** automatically cross-references the vulnerability the threat is targeting with the targeted machine or device to determine if it is vulnerable to that threat. Accuracy and efficiencies are realized, and the need to layer more and more point products is reduced. Subsequently, the costs to acquire, operate, and manage the additional multiple point products are also reduced. The platform will also remotely remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented. Page 9 of Annex A. For example, if the attack is a Window based attack targeting a Windows machine. Is the targeted machine actually running Windows, and if so, is the machine vulnerable to the attack? Lastly, if so, the targeted vulnerability remains unremediated – the IDS system can not remediate it. Page 16 of Annex A. ***Logic Engine*** The logic engine, or system intelligence, cross references the vulnerability the threat is targeting and the targeted machine or device vulnerabilities through the data warehouse, and returns the answer to the point product. It also determines which updates are needed and compatible with each machine's configuration. The logic engine cross-references and matches each client's configuration with the information for each update, and determines which updates are appropriate. It then takes these results and filters them through the group policy to determine which updates should actually be installed on the client. Lastly the logic engine once more references the group policy to determine what action (if any) to take, and then performs this action at the appropriate time. Page 20 of Annex A.

System Requirements

There are two system requirements: TCP/IP connectivity, and supported network r and devices. Platforms supported are:

- All Windows Operating Systems and their applications
- All UNIX variants
- Cisco routers and firewalls
- Linksys network devices
- Netgear network devices
- Toshiba network devices

Platform support is scalable to any network size or architecture; consumer, small offi office (SOHO), enterprise, and distributed networks.

What is the SDK and Anti-Vulnerability Platform ?

The SDK was designed to be a simple integration pathway to the back-end Anti-Vulnerability platform - consisting of a logic engine and vulnerability data warehouse. It will enable any network security product such as an IDS, scanner, or firewall to intelligently reference and share the same vulnerability data set, and provide complete vulnerability remediation functionalities. Thereby, improving system accuracy and efficiencies, minimizing false positives and false negatives, and providing policy compliance and enforcement capabilities.

A product architect simply chooses the functionality desired, inserts the provided functionality SDK sample code into the product code. (Detailed in a separate document, titled: *SDK User's Guide*.) The SDK sample code will then query --via the logic engine - the Anti-Vulnerability data warehouse, and in turn will return an answer to the point product. The architect can then show the results in any format desired in the product's interface. Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well.

Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience.

Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy - increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance functionality.

Page 5-6 of Annex A.

See also the functions on pages 12-15 of Annex A.

C

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence	**What is the SDK and Anti-Vulnerability Platform?** The SDK was designed to be a simple integration pathway to the back-end Anti-Vulnerability platform - consisting of a logic engine and vulnerability data warehouse. It will enable any network security product such as an IDS, scanner, or firewall to intelligently reference and share the same vulnerability data set, and provide complete vulnerability remediation functionalities. Thereby, improving system accuracy and efficiencies, minimizing false positives and false negatives, and providing policy compliance and enforcement capabilities. Page 3 of Annex A. **SDK Applications - Example Product Integration** Examples of additional functionalities that may be integrated into point products via the SDK for enterprise and small office home office (SOHO) networks: 1. Patch Deployment – Remotely remediates network vulnerabilities and provides policy compliance and enforcement capabilities. See SecurityProfiling's SysUpdate white paper and trial download online. 2. IDS –Eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities. 3. Scanner - Eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities. 4. Firewall - Eliminates false positive and false negatives, preventing the security system from denying valid traffic to the organization - self-inflicted denial of service attacks, and adds vulnerability remediation, and policy compliance and enforcement functionalities. 5. Vulnerability Management – Same as 1., above. 6. Multiple Products: IDS, Scanner, and Firewall - Each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats. 7. Client Security - Attain the additional functionalities and benefits as the multiple products listed above, yet are even more effective since they additionally communicate and share information directly with each other. They will also attain vulnerability identification, reference, remediation, and policy compliance and enforcement capabilities. Page 4 of Annex A.

mitigation types across the plurality of devices;	**What is the SDK and Anti-Vulnerability Platform ?** The SDK was designed to be a simple integration pathway to the back-end Anti-Vulnerability platform - consisting of a logic engine and vulnerability data warehouse. It will enable any network security product such as an IDS, scanner, or firewall to intelligently reference and share the same vulnerability data set, and provide complete vulnerability remediation functionalities. Thereby, improving system accuracy and efficiencies, minimizing false positives and false negatives, and providing policy compliance and enforcement capabilities. A product architect simply chooses the functionality desired, inserts the provided functionality SDK sample code into the product code. (Detailed in a separate document, titled: *SDK User's Guide*.) The SDK sample code will then query --via the logic engine - the Anti-Vulnerability data warehouse, and in turn will return an answer to the point product. The architect can then show the results in any format desired in the product's interface. Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well. Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience. Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy - increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance functionality. Page 6 of Annex A. 2. IDS IDS products attempt to identify malicious code by signatures at both the network and host client level based. While they may be able to identify its CVE ID or other vulnerability identifier, and target, they generally do not have the intelligence to determine if the any of the machines on the network are susceptible to that attack, or with finer granularity, if any machine has a specific vulnerability to that specific attack. For example, if the attack is a Window based attack targeting a Windows machine. Is the targeted machine actually running Windows, and if so, is the machine vulnerable to the attack? Lastly, if so, the targeted vulnerability remains unremediated -- the IDS system can not remediate it. Benefits: With the SDK, a product architect can integrate functionalities listed in the previous section to enable the IDS to access the anti-vulnerability logic engine and platform. It will then have the intelligence to determine if any machine on the network is susceptible to the attack, remediate the vulnerability, mitigate the attack, and verify policy compliance. Now, if no machines were susceptible to the attack, the code is identified as a false positive, no further data or alert is generated, and a management response is not required. With the SDK and platform, the product will gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks. Page 16 of Annex A.

	4. Firewall "Smart" firewalls are based in part on signatures and other similar functionalities as IDS products described above. With the SDK and platform the firewall can determine whether an attack is valid or a false positive, thereby preventing the security system from denying valid traffic to the organization - self-inflicted DoS attacks. Such functionalities and benefits are available for both the enterprise and SOHO networks. **5. Vulnerability Management** Vulnerability Management products enable managers to set policy and identify potential network vulnerabilities. They typically do not accurately identify each vulnerability on each network machine and device, nor remediate each vulnerability, meeting policy compliance enforcement requirements. Benefits: The SDK and platform offer similar functionalities and benefits as the patch deployment products described above. In short, it enables products to add accurate vulnerability identification, remediation, verification, and policy compliance. Such functionalities and benefits are available for both the enterprise and SOHO networks. **6. Multiple Products: IDS, Scanner, and Firewall** Each product functions as the individual products noted above. Each may be deployed and operate on the network in a multi-tiered network defense strategy. They may be disparate system, and their signatures and update deployment schedules may vary. Therefore, the probability of mitigating a new and complex threat decreases, while management requirements and cost increases. Benefits: With the SDK and platform, they each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats. Page 17 of Annex A.

ForcePoint LLC
EX-1002
Page331

wherein the at least one configuration involves at least one operating system.	**Functional Description** 1. **Integrates point products and provides system intelligence.** The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats. 2. **Cross-references the vulnerability targeted by the threat.** The vulnerability targeted by the threat is attained by the point products and the CVE ID or other identifier is fed into the logic engine where it is cross-referenced with the vulnerabilities of the targeted machine. An answer is returned accurately indicating if the machine is vulnerable. 3. **Identifies network vulnerabilities.** The platform will independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly. Page 3 of Annex A. The platform's enables point products to share information via its proprietary **logic engine** automatically cross-references the vulnerability the threat is targeting with the targeted machine or device to determine if it is vulnerable to that threat. Accuracy and efficiencies are realized, and the need to layer more and more point products is reduced. Subsequently, the costs to acquire, operate, and manage the additional multiple point products are also reduced. The platform will also remotely remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented. Page 9 of Annex A. For example, if the attack is a Window based attack targeting a Windows machine. Is the targeted machine actually running Windows, and if so, is the machine vulnerable to the attack? Lastly, if so, the targeted vulnerability remains unremediated – the IDS system can not remediate it. Page 16 of Annex A.

	Client Agent The agent is remotely deployed to each machine or device on the network, and has two primary functions. 1. Accurately identifies the OS, applications, firmware, and updates installed on each machine or device. 2. Installs the updates. ***Identifies Applications Installed*** The client agent accurately identifies and inventories the operating system, applications, and updates installed on each machine. Periodically, the on-site server polls each client agent and the configuration data is transferred back to the server. The logic engine determines and deploys the appropriate updates to each machine. (More detail of this process is provided in the next sub-section, – Logic Engine.) Page 19 of Annex A.
	It should be strongly noted that above exemplary non-exhaustive excerpts are set forth for illustrative purposes only and should not be construed as limiting in any manner whatsoever to the claims.

ForcePoint LLC
EX-1002
Page333

Electronic Patent Application Fee Transmittal	
Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	650	650
STATUTORY OR TERMINAL DISCLAIMER	2814	1	160	160
		Total in USD ($)		**910**

Electronic Acknowledgement Receipt	
EFS ID:	35219706
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	21-FEB-2019
Filing Date:	30-MAY-2017
Time Stamp:	22:15:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$910
RAM confirmation Number	022219INTEFSW22160600
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SP1P012C_RCE_vF_21-Feb-2019.pdf	1349611 36c3e513a07f70aa7f1dc1c096382df90e509da5	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	SP1P012C_AmendmentB_RCE_vF_21-Feb-2019.pdf	71651 44705dddf9538b81d8fe1aa32a47721c7720f77b	no	5
Warnings:					
Information:					
3	Affidavit-Rule 131-pre-AIA (FTI) ONLY	SP1P0012C_Affidavit_02_2019_JB.pdf	701062 25fe78d0449dc11efd4a9b541364d43b4ad79473	no	2
Warnings:					
Information:					
4	Examination support document	Annex_A.pdf	3736204 1fa392ba0b9a3c952fe4757181b10c52ad41ad62	no	32
Warnings:					
Information:					
5	Examination support document	SP1P012C_Annex_B.pdf	3331657 145df962e9e3130a11b6b2de2dd5eea3f81b3b07	no	11
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	34025 032a5de8365e7565217f46053ad475770aeaf8f5	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	9224210

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: February 21, 2019

AMENDMENT B
AND
REQUEST FOR CONTINUED EXAMINATION

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 11/05/18, please enter the following amendments

C

ForcePoint LLC
EX-1002
Page339

Remarks:

Claims 21-24 and 26-58 are provisionally rejected on the ground of non-statutory double patenting as being unpatentable over claims 21-46 of co-pending Application No. 15/608,981. Such rejection is deemed avoided by virtue of the terminal disclaimer filed concurrently herewith.

Claims 21, 26, and 31 are rejected under 35 U.S.C. 112(B) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Specifically, the Examiner points out that Claim 21 has been amended to recite first vulnerability information and second vulnerability information, and that the claim also recites accurately identified vulnerability and potential vulnerability, but then alleges that it is unclear whether these phrases are the same as first and second vulnerabilities or different.

Applicant respectfully disagrees with this rejection. The claims specifically set forth the relationship between the "first vulnerability **information**", the "second vulnerability **information**", the "plurality of **potential vulnerabilities**", and/or the "at least one **accurately identified vulnerability**" (emphasis added). Just by way of example, Claim 21 states that the "second vulnerability **information** … is used to identify a plurality of **potential vulnerabilities**" and the "**first** vulnerability **information** [is] generated utilizing the **second** vulnerability **information**, by: … determining that the plurality of devices is vulnerable to **at least one accurately identified vulnerability** (emphasis added), in the specific context claimed. Thus, it is clear from the claims as to the relationship between the relevant terms.

The Examiner goes on to argue that the specifications do not cite determining whether a device is vulnerable based on potential vulnerabilities. The Examiner alleges that the phrase "potential" indicates that a vulnerability has the potential to [be] a vulnerability but [is] not guaranteed to be a vulnerability. The Examiner further alleges that the specifications show

C

ForcePoint LLC
EX-1002
Page340

support for determining that a device is vulnerable to a vulnerability based on vulnerabilities shared amongst various device but does not show proper support for determining that a device is vulnerable to a vulnerability based on "potential vulnerabilities".

Applicant respectfully disagrees with this rejection. As mentioned earlier, the specifications disclose that "a product architect can integrate functionalities listed in the previous section to enable the scanner to access the logic engine and platform, and then have the intelligence to determine if the machine has **actual vulnerabilities**, remediate them, and verify policy compliance" (emphasis added). In order to identify such "**actual**" vulnerabilities, the specifications disclose that "the platform enables network security products to share information via its proprietary logic engine to automatically **cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat**" and further discloses that "**it may cross-reference the threat's identifier with the target's configuration**. The **threat's CVE** [Common Vulnerabilities and Exposures] **ID, or other identifier**, and the destination IP address are fed into the logic engine **where it cross-references the threat with the machine's existing OS, application, and patch configuration profile**. **An answer is returned accurately indicating if the machine is vulnerable.**" (emphasis added).

Thus, as to Claim 21, the aforementioned **Common** Vulnerabilities and Exposures (CVE) "identifier" is one of multiple exemplary disclosures related to the identification of a "potential vulnerability" which, as disclosed above, may clearly be used for "determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities," in the specific context claimed. Again, it should be noted that such non-exhaustive exemplary support is set forth for illustrative purposes only, and such citations (and any context thereof) should not be construed as limiting to claims in any manner. As to Claims 26 and 31, such claims are deemed allowable for similar (but not necessarily identical) reasons (see such claims for terms used therein).

C

ForcePoint LLC
EX-1002
Page341

Claims 21-24, 26, 27, 31-33, 37-2, 45, 46, 50-52 and 55-57 are rejected under pre-AIA 35 U.S.C. 1 03(a) as being unpatentable over prior art of record US 7257630 to Cole et al (hereinafter Cole), prior art of record US 20050193430 to Cohen et al (hereinafter Cohen) and US 6550012 to Villa et al (hereinafter Villa).

In response, it is noted that Cohen indicates an earliest effective filing date of October 1, 2002. As shown by the attached Declaration of John Blignaut Under 37 CFR § 1.131, the claimed invention was conceived and reduced to practice prior to the effective date of the Cohen reference. This fact excludes the Cohen reference from the body of prior art under 35 USC § 102(e). In view of such declaration and supporting evidence, the foregoing rejections are deemed to have been overcome.

It is believed that all of the pending issues have been addressed. The claims are in condition for allowance. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, it should be noted that no claim is intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-4964 (Order No. SP1P012C).

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

C

ForcePoint LLC
EX-1002
Page342

Respectfully submitted,



Dated: 21 Feb 2019

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page343

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/608,978	Filing Date 05/30/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	02/21/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 27	Minus	** 45	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/SHERRY A DAVIS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 05/08/2019

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER
HERZOG, MADHURI R

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
05/08/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

Office Action Summary	**Application No.** 15/608,978	**Applicant(s)** Oliphant et al.	
	Examiner MADHURI R HERZOG	**Art Unit** 2438	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 02/21/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 21-24 and 26-59 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 21-24 and 26-59 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 11/14/2018.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 21-24 and 26-59 have been examined.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/21/2019 has been entered.

Terminal Disclaimer

4. The terminal disclaimer filed on 02/21/2019 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **any patent granted on Application Number 15/608981** has been reviewed and is accepted. The terminal disclaimer has been recorded.

ForcePoint LLC
EX-1002
Page347

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 11/14/2018 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Amendment

6. Applicant's arguments filed on 02/21/2019 with regards to rejection of claims 21, 26 and 31 under 35 U.S.C 112 have been fully considered but they are not persuasive. Claims 21, 26 and 31 recite the limitations: "first vulnerability information", "second vulnerability information", "accurately identified vulnerability" and "potential vulnerability". The use of the different terminology to indicate the various vulnerabilities has decreased the clarity of the claims.

7. Applicant's arguments with respect to claims 21, 26 and 31 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 21-24 and 26-59 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more. The claims recite, receiving first vulnerability information from a database, identifying a configuration that

ForcePoint LLC
EX-1002
Page348

includes an operating system associated with the plurality of devices, generating first vulnerability information associated with a plurality of devices by utilizing the configuration of the devices along with second vulnerability information retrieved from a database, identifying an occurrence, determining if at least one device is susceptible to the occurrence based on the first vulnerability information and allowing selective utilization of mitigation actions including a firewall-based and intrusion prevention based mitigation type.

The limitations of receiving first vulnerability information from a database, identifying the configuration including the operating system of the devices and generating first vulnerability information by utilizing the configuration of the devices and second vulnerability information, as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitations in the mind but for the recitation of generic computer components. That is, other than reciting "one or more processors to," nothing in the claim element precludes the step from practically being performed in the mind. For example, but for the "one or more processors to" language, "receiving", "identifying" and "generating" in the context of this claim encompasses the user manually performing the steps. Similarly, the limitations of identifying an occurrence, determining if at least one device is susceptible to the occurrence based on the first vulnerability information and allowing selective utilization of mitigation actions including a firewall-based and intrusion prevention based mitigation type as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitations in the mind but for the recitation of generic computer components. For example, but for the "one or more processors to" language, "identifying", "determining"

ForcePoint LLC
EX-1002
Page349

and "allowing" in the context of this claim encompasses the user manually identifying an occurrence, manually determining that at least one device is susceptible to the occurrence based on the first vulnerability information and manually selecting a mitigation action. If a claim limitation, under its broadest reasonable interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components, then it falls within the "Mental Processes" grouping of abstract ideas. Accordingly, the claim recites an abstract idea.

This judicial exception is not integrated into a practical application. In particular, the claim only recites one additional element – using a processor to perform all the steps. The processor in all the steps is recited at a high-level of generality (*i.e.*, as a generic processor performing a generic computer function) such that it amounts no more than mere instructions to apply the exception using a generic computer component. Accordingly, this additional element does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea. The claim is directed to an abstract idea.

The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception. As discussed above with respect to integration of the abstract idea into a practical application, the additional element of using a processor to perform all the steps amounts to no more than mere instructions to apply the exception using a generic computer component. Mere instructions to apply an exception using a generic computer component cannot provide an inventive concept. The claim is not patent eligible.

ForcePoint LLC
EX-1002
Page350

Similarly, the dependent claims 22-24, 27-30 and 32-59 are directed to an abstract idea.

Claim Rejections - 35 USC § 112

9. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 21, 26 and 31 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Claims 21, 26 and 31 recite the limitations: "first vulnerability information", "second vulnerability information", "accurately identified vulnerability" and "potential vulnerability". The use of the different terminology to indicate the various vulnerabilities has made the claims unclear. To improve the clarity of the claims, the examiner suggests using consistent language throughout the claims.

Claim Rejections - 35 USC § 103

11. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

ForcePoint LLC
EX-1002
Page351

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 21, 24, 26, 27, 31-33, 37, 38, 40, 41, 45, 46, 51 and 55-57 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7181769 to Keanini et al (hereinafter Keanini) and US 7509681 to Flowers et al (hereinafter Flowers).

As per claims 21 and 26, Keanini teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Keanini: column 12, lines 1-27: The control module 320 identifies 1050 the total set of vulnerabilities for the host 191 from the vulnerability trees. Next, the control module 320 uses the sensors 345, 355 to verify 1060 the existence of the vulnerabilities on the host 191)**;

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential

ForcePoint LLC
EX-1002
Page352

vulnerabilities **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Also, column 10, lines 59-67 and column 12, lines 1-27)**;

identify an occurrence in connection with at least one of the plurality of devices **(Keanini: column 11, lines 53-65: The traffic sniffing module 840 monitors network traffic to detect traffic corresponding to attack signatures in the attack signatures module 920. The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures);**

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information **(Keanini: column 11, lines 53-65: Preferably, the traffic sniffing module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic)**; and

**ForcePoint LLC
EX-1002
Page353**

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs)**;

wherein the at least one configuration involves at least one operating system **(Keanini: column 7, lines 20-25: The low-level sensor 345 identifies operating systems running on hosts 191 and/or other characteristics)**.

Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach an intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

an intrusion prevention system-based occurrence mitigation type **(Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the**

ForcePoint LLC
EX-1002
Page354

user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Flowers in the invention of Keanini to include an intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to not only allow an intrusion detection system (IDS) to leverage off the information gathered by the vulnerability detection system (VDS) but also allows a simple way to define rules for use by the vulnerability and intrusion detection systems to check for network conditions, such as vulnerabilities or intrusions (Flowers: column 2, lines 23-30).

As per claim 24, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating**

ForcePoint LLC
EX-1002
Page355

system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Column 9, lines 35-67: The vulnerability tree for operating systems is similar to the application vulnerability tree 400 described above. For example, a top level of the tree can represent an operating system family (e.g., Unix, Windows, and MacOS) and descending levels can represent specific operating systems in each family (e.g., specific to Widows is XP, NT, 2000), operating system versions (e.g., specific to NT is 3.5 and 4.0), and patch levels (specific to 3.5 is Service Pack 1 and Service Pack 2). Also, column 10, lines 59-67 and column 12, lines 1-27).

As per claim 31, Keanini teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Keanini: column 12, lines 1-27: The control module 320 identifies 1050 the total set of vulnerabilities for the host 191 from the vulnerability trees. Next, the control module 320 uses the sensors 345, 355 to verify 1060 the existence of the vulnerabilities on the host 191)**;

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Also, column 10, lines 59-67 and column 12, lines 1-27)**;

display information that is based on the first vulnerability information **(Pearson: column 10, lines 3-23: The network profiling module 620 stores the information used by device profilers 165 to identify vulnerabilities and also stores the vulnerabilities of the system 100 detected by the device profilers 165. In one**

ForcePoint LLC
EX-1002
Page357

embodiment, the network profiling module 620 generates an abstract view of the configuration of the enterprise network 115 from the information collected from the individual device profilers 191);

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs)**; and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices **(Keanini: column 11, lines 53-65: The traffic sniffing module 840 monitors network traffic to detect traffic corresponding to attack signatures in the attack signatures module 920. The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures)**;

wherein the at least one configuration involves at least one operating system **(Keanini: column 7, lines 20-25: The low-level sensor 345 identifies operating systems running on hosts 191 and/or other characteristics)**.

Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach an intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

an intrusion prevention system-based occurrence mitigation type **(Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Flowers in the invention of Keanini to include an intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to not only allow an intrusion detection system (IDS) to leverage off the information gathered by the vulnerability detection system (VDS) but also allows a simple way to define rules for use by the vulnerability and intrusion detection systems to check for network conditions, such as vulnerabilities or intrusions (Flowers: column 2, lines 23-30).

As per claims 27, 33 and 41, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation

ForcePoint LLC
EX-1002
Page359

actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs. Flowers: column 3, line 55-column 4, line 15: Thus, an IDS 116 used with an embodiment of the invention examines network traffic for signs of malicious activity. However, the rules loaded are determined by the VDS vulnerability analysis, so that only rules that describe possible intrusion conditions as they exist for the specific network 100 are loaded. So if a vulnerability V is identified, the intrusion detection system is target-based by virtue of the fact that it monitors**

ForcePoint LLC
EX-1002
Page360

the system running with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V).

As per claims 32 and 38, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence **(Keanini: column 11, lines 15-33: In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

As per claim 37, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation **(Flowers: Abstract: The intrusion detection system leverages off of information**

ForcePoint LLC
EX-1002
Page361

gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64).

As per claim 40, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one accurately identified vulnerability **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820**

ForcePoint LLC
EX-1002
Page362

responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs).

As per claim 45, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: determine the occurrence to have a first severity if it is determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence; determine the occurrence to have a second severity if it determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is not susceptible to being taken advantage of by the occurrence; and report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity **(Keanini: column 2, lines 55-67: A traffic monitor monitors network traffic for attack signatures corresponding to the determined vulnerabilities to detect malicious activity. In one embodiment, the traffic monitor associates attack signatures with the specific destination (e.g., IP address and/or port) having the corresponding vulnerability. The traffic monitor does not signal an attack unless the attack matches the attack signature of an exploit of a vulnerability and is directed to a destination known to have the vulnerability. Column 11, lines 53-65:**

ForcePoint LLC
EX-1002
Page363

Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Additionally, the traffic sniffing module 930 is configured to send a notification message to the centralized correlation server 175 in response to detecting an attack signature. Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked).

As per claim 46, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action **(Keanini: Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked. In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Column 2, lines 43-**

ForcePoint LLC
EX-1002
Page364

62: The rules used by the VDS and IDS are easily formed and therefore, an end user, such as a security or network engineer, can easily define and construct rules beyond any that are defined by the VDS/IDS provider).

As per claim 51, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one accurately identified vulnerability while there is no installation of a patch that removes the at least one accurately identified vulnerability **(Keanini: Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked. In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Column 2, lines 43-62: The rules used by the VDS and IDS are easily formed and therefore, an end user, such as a security or network engineer, can easily define and construct rules beyond any that are defined by the VDS/IDS provider)**.

As per claim 55, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions

**ForcePoint LLC
EX-1002
Page365**

for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused **(Keanini: column 2, lines 29-37: The control module determines a set of potential vulnerabilities by summing the vulnerabilities at each traversed node. The control module determines whether the vulnerabilities actually exist on the host and sends a list of the verified vulnerabilities to the centralized correlation server. Column 11, lines 53-65: The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures. Preferably, the traffic sniffing module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic. Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Column 12, lines 52-67: In response to receiving 1210 a notification related to vulnerabilities sent by the device profiler 165, the event daemon module 820 performs a set of actions such as configuring 1220 the firewall 150 to prevent the attack)**.

As per claim 56, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence **(Keanini: Column 11, lines 53-65: The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures. Preferably, the traffic sniffing**

ForcePoint LLC
EX-1002
Page366

module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic. Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Column 12, lines 52-67: In response to receiving 1210 a notification related to vulnerabilities sent by the device profiler 165, the event daemon module 820 performs a set of actions such as configuring 1220 the firewall 150 to prevent the attack).

As per claim 57 Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system- based occurrence mitigation type being selectively caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence **(Keanini: column 11, lines 15-33: In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191,**

ForcePoint LLC
EX-1002
Page367

and/or preventing the operating systems and/or applications from executing programs. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64).

14. Claims 22, 23, 28-30, 34-36, 39, 42, 44, 47-50, 52-54, 58 and 59 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Keanini in view of Flowers as applied to claim 21, 26 and 31 above, and further in view of US 20050235360 to Sterling Michael Pearson (hereinafter Pearson).

As per claim 22, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by

ForcePoint LLC
EX-1002
Page368

sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device. However, Pearson teaches:

wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level**

ForcePoint LLC
EX-1002
Page369

may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the

ForcePoint LLC
EX-1002
Page370

particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 23, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured such that at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device. However, Flowers teaches:

wherein the instructions are configured such that at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request

ForcePoint LLC
EX-1002
Page371

across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that

ForcePoint LLC
EX-1002
Page372

at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 28, 34 and 58, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input,

ForcePoint LLC
EX-1002
Page373

automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions, when executed by the

ForcePoint LLC
EX-1002
Page374

one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 29 and 35, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence. However, Flowers teaches:

ForcePoint LLC
EX-1002
Page375

wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed**

ForcePoint LLC
EX-1002
Page376

embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 30 and 36, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for

ForcePoint LLC
EX-1002
Page377

selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to**

ForcePoint LLC
EX-1002
Page378

certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely

ForcePoint LLC
EX-1002
Page379

configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 39, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only relevant occurrence mitigation actions are available for selection by the user **(Flowers: column 4, lines 1-15: Such a Target-based IDS will have the ability to monitor for specific conditions to which the network has been determined to be vulnerable, as well as any range of conditions or attacks to which the network might be vulnerable. For instance, if the VDS finds a type of service S, but has not verified S's vulnerability to a buffer overflow condition, the IDS may still monitor for such a buffer overflow. So if a vulnerability V is identified, the intrusion detection system is target-based by virtue of the fact that it monitors the system running with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V)**.

Keanini in view of Flowers does not explicitly teach: one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user. However, Pearson teaches:

one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user **(Pearson: [0063] The user**

ForcePoint LLC
EX-1002
Page380

may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 42, Keanini in view of Flowers teaches reporting of the occurrence but does not explicitly teach: wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based

ForcePoint LLC
EX-1002
Page381

occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device. However, Pearson teaches:

wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that

ForcePoint LLC
EX-1002
Page382

additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 44, Keanini in view of Flowers does not teach: wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability. However, Pearson teaches:

wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio**

ForcePoint LLC
EX-1002
Page383

buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 47, Keanini in view of Flowers does not teach: wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface

ForcePoint LLC
EX-1002
Page384

of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options. However, Pearson teaches:

wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to**

ForcePoint LLC
EX-1002
Page385

certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options. The motivation to do so would be to

ForcePoint LLC
EX-1002
Page386

remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 48, Keanini in view of Flowers does not teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Pearson teaches:

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence

ForcePoint LLC
EX-1002
Page387

mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a

ForcePoint LLC
EX-1002
Page388

second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 49, Keanini in view of Flowers and Pearson teaches:

The non-transitory computer-readable media of Claim 48, wherein the instructions are configured such that the automatic application of the first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type includes sending a second signal to at least one component with intrusion prevention system functionality **(Keanini: column 12, lines 52-67: In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-67 and column 4, lines 1-15: So if a vulnerability V is identified, the intrusion detection**

ForcePoint LLC
EX-1002
Page389

system is target-based by virtue of the fact that it monitors the system running with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V).

As per claim 50, Keanini in view of Flowers does not teach: wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences. However, Pearson teaches:

wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences (**Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high**

ForcePoint LLC
EX-1002
Page390

security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 52, Keanini in view of Flowers teaches:

**ForcePoint LLC
EX-1002
Page391**

The non-transitory computer-readable media of Claim 21, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device **(Keanini: column 11, lines 53-65)**; the determining that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine whether a first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet **(Keanini: column 11, lines 53-65. Flowers: column 3, line 55-column 4, line 15)**, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one second occurrence packet **(Keanini: column 11, lines 53-65. Flowers: column 3, line 55-column 4, line 15)**; and the allowing the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface **(Keanini: column 11, lines 15-25 and column 10, lines 3-10. Flowers: column 2, lines 42-47)**; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed by sending a first signal over at least one network to a first

ForcePoint LLC
EX-1002
Page392

component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device **(Keanini: column 12, lines 52-67)**; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type is completed by sending a second signal to a second component with an intrusion prevention system type functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device **(Flowers: column 3, line 55-column 4, line 15)**.

Keanini in view of Flowers does not explicitly teach based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed. However, Pearson teaches:

based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received**

ForcePoint LLC
EX-1002
Page393

from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 53, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 52, wherein the instructions are configured such that at least one of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Keanini: column 5, lines 26-33)**; said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith **(Keanini: column 12, lines 40-52)**; said first vulnerability information is generated via a vulnerability scan operation **(Keanini: column 7, lines 1-7)**; said first device, said second device, and said third device are part of the same group **(Keanini: column 4, lines 5-25)**; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status **(Keanini: column 10, lines 5-10)**; said at least one configuration

ForcePoint LLC
EX-1002
Page394

includes at least one of a configuration option, a policy setting, or a patch **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration is identified via user input in connection with at least one setting **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability **(Keanini: column 12, lines 52-67)**; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Keanini: column 12, lines 52-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Flowers: Abstract, column 3, line 55-column 4, line 15)**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-**

67); said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said at least one accurately identified vulnerability includes the at least one operating system **(Keanini: column 9, lines 45-65)**; said actual vulnerabilities include the at least one accurately identified vulnerability **(Keanini: column 2, lines 4-16)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of

devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which includes the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; said different occurrence mitigation actions include different remediation actions **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Keanini: column 11, lines 43-65)**; said at least one aspect of the at least one first occurrence packet involves at least one of a payload thereof or an IP address **(Keanini: column 11, lines 43-65)**; said at least one aspect of the at least one first occurrence packet is utilized to determine whether the first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet,

ForcePoint LLC
EX-1002
Page397

by utilizing the at least one aspect in connection with at least one of a cross-referencing operation or a look-up operation **(Keanini: column 11, lines 43-65)**; said first signal and the second signal include at least one of response signals, or signals sent in response to a query signal **(Keanini: column 11, lines 43-65 and column 12, lines 52-67)**; said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality **(Keanini: column 12, lines 52-67)**; said second component with the intrusion prevention system type functionality includes at least one of an intrusion prevention system, an intrusion detection system with the intrusion prevention system type functionality, a gateway with the intrusion prevention system type functionality, a router with the intrusion prevention system type functionality, a sensor with the intrusion prevention system type functionality, or a multiple-security product system with the intrusion prevention system type functionality **(Flowers: column 3, lines 55-67)**; said preventing includes at least one of rejecting a request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or said automatic response includes a real-time response **(Keanini: column 12, lines 52-67)**.

Keanini in view of Flowers does not teach: said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. However, Pearson teaches:

ForcePoint LLC
EX-1002
Page398

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 54 and 59, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of: said at least one first data storage includes at least one first database; said at least one second data storage includes at

ForcePoint LLC
EX-1002
Page399

least one second database **(Keanini: column 5, lines 26-33)**; said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith **(Keanini: column 12, lines 40-52)**; said first vulnerability information is generated via a vulnerability scan operation **(Keanini: column 7, lines 1-7)**; said first vulnerability information identifies at least one actual vulnerability **(Keanini: column 2, lines 4-16)**; said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities **(Keanini: column 5, lines 25-40)**; said first device, said second device, and said third device are part of the same group **(Keanini: column 4, lines 5-25)**; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration is utilized for identifying the at least one operating system or an application **(Keanini: column 7, lines 20-25)**; said at least one configuration is identified utilizing information regarding the at least one operating system or an application **(Keanini: column 7, lines 20-25)**; said at least one configuration is identified via user input in connection with at least one setting **(Keanini: column 10, lines 5-10)**; said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability; said firewall-based occurrence mitigation type includes at least one of: a

ForcePoint LLC
EX-1002
Page400

type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Keanini: column 12, lines 52-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Flowers: Abstract, column 3, line 55-column 4, line 15)**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the

ForcePoint LLC
EX-1002
Page401

different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said at least one actual vulnerability is the at least one operating system **(Keanini: column 9, lines 45-65)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence

ForcePoint LLC
EX-1002
Page402

mitigation actions of the diverse occurrence mitigation types **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said different occurrence mitigation actions include different remediation actions; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Keanini: column 11, lines 43-65)**; said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration **(Keanini: column 2, lines 29-37, column 20-65)**; said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software **(Keanini: column 7, lines 8-46)**; said determining that the plurality of devices is actually vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration **(Keanini: column 7, lines 49-67 and column 8, lines 27-56)**; said non-transitory computer-readable media includes a single non-transitory computer readable medium; one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time; one or more of said different occurrence mitigation actions, after

an automatic application thereof, is utilized at a later time for the occurrence mitigation **(Keanini: column 12, lines 52-67. Flowers: column 3, lines 55-67)**; one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch **(Flowers: column 3, lines 55-67)**; one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component **(Keanini: column 12, lines 52-67)**; and wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation **(Keanini: column 12, lines 52-67)**, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices **(Keanini: column 7, lines 8-46)**.

Keanini in view of Flower does not explicitly teach: one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; and to deploy a patch. However, Pearson teaches:

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high**

ForcePoint LLC
EX-1002
Page404

security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049]);

to deploy a patch **(Pearson: Based upon the received status information, the remote computer then determines whether the communication device requires a software update. If the device requires such a software update, the remote computer queues any necessary software patches for later download to the communication device. Also, [0044])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; and to deploy a patch. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

15. Claim 43 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Keanini in view of Flowers as applied to claim 41 above, and further in view of prior art of record US 20030126472 to Carl Banzhof (hereinafter Banzhof).

As per claim 43, Keanini in view of Flowers does not teach: wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results

ForcePoint LLC
EX-1002
Page405

in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. However, Banzhof teaches:

wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device (Banzhof: [0031]: In box 86, the client user, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability does not pose a sufficient security risk, the remediation signature is deemed too risky, etc. [0032]: If the remediation is not deemed successful, either because it did not resolve the identified vulnerabilities as evidenced by an additional security scan of the client computer, or because the remediation actions had unintended deleterious effects, etc., then the remediation can be rolled back or undone and the remediation process can be repeated as indicated in box 99).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Keanini in view of Flowers to include wherein the instructions are configured

ForcePoint LLC
EX-1002
Page406

such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 7712138 to Zobel et al: Once the system runs the security audit, a vulnerability assessment can be calculated for each element in the network. The vulnerability assessment can be presented in a format that facilitates interpretation and response by someone operating the system. The vulnerability assessment can also be used to configure and schedule future security audits.

US 6301699 to Hollander et al: Method for detecting buffer overflow weakness exploitation, including the steps of determining a plurality of threshold parameters, each respective to a buffer overflow weakness exploitation event, analyzing a code to be executed, thereby producing a plurality of validation values, comparing said validation values to the respective ones of the threshold parameters, and determining a buffer overflow weakness exploitation attempt, when at least one of the validation values exceeds the respective one of the threshold parameters.

ForcePoint LLC
EX-1002
Page407

US 6415321 to Gleichauf et al: A method and system for mapping a network domain provides a centralized repository for network information to support network devices, including an intrusion detection system.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI R HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on 8:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ForcePoint LLC
EX-1002
Page408

MADHURI R. HERZOG
Primary Examiner
Art Unit 2438

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1002
Page409

Notice of References Cited	Application/Control No. 15/608,978	Applicant(s)/Patent Under Reexamination Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7509681-B2	03-2009	Flowers; John S.	G06F21/552	713/151
*	B	US-7712138-B2	05-2010	Zobel; Robert David	G06F21/577	709/224
*	C	US-7181769-B1	02-2007	Keanini; Timothy D.	H04L63/1416	713/166
*	D	US-6301699-B1	10-2001	Hollander; Yona	G06F21/55	717/131
*	E	US-6415321-B1	07-2002	Gleichauf; Robert E.	H04L41/00	709/224
*	F	US-20050235360-A1	10-2005	Pearson, Sterling Michael	H04L29/06	726/23
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019						
	1	-	-	-						
	2	-	-	-						
	3	-	-	-						
	4	-	-	-						
	5	-	-	-						
	6	-	-	-						
	7	-	-	-						
	8	-	-	-						
	9	-	-	-						
	10	-	-	-						
	11	-	-	-						
	12	-	-	-						
	13	-	-	-						
	14	-	-	-						
	15	-	-	-						
	16	-	-	-						
	17	-	-	-						
	18	-	-	-						
	19	-	-	-						
	20	-	-	-						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23	✓	✓	✓						
	24	✓	✓	✓						
	25	✓	-	-						
	26	✓	✓	✓						
	27	✓	✓	✓						
	28	✓	✓	✓						
	29	✓	✓	✓						
	30	✓	✓	✓						
	31	✓	✓	✓						
	32	✓	✓	✓						
	33	✓	✓	✓						
	34	✓	✓	✓						
	35	✓	✓	✓						
	36	✓	✓	✓						
	37	✓	✓	✓						
	38		✓	✓						
	39		✓	✓						
	40		✓	✓						
	41		✓	✓						
	42		✓	✓						

C

ForcePoint LLC
EX-1002
Page411

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019						
	43		✓	✓						
	44		✓	✓						
	45		✓	✓						
	46		✓	✓						
	47		✓	✓						
	48		✓	✓						
	49		✓	✓						
	50		✓	✓						
	51		✓	✓						
	52		✓	✓						
	53		✓	✓						
	54		✓	✓						
	55		✓	✓						
	56		✓	✓						
	57		✓	✓						
	58		✓	✓						
	59		✓	✓						

ForcePoint LLC
EX-1002
Page412

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

CPC - Searched*		
Symbol	Date	Examiner
H04L 63/02$, 63/14$, 63/20$	05/03/2019	M.H
G06F 21/5$	05/03/2019	M.H

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search, Assignee search	05/03/2019	M.H
East search	05/03/2019	M.H

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page413

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S20	152	"6952779"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/05/01 15:52
S21	36	("4773028" | "5032979" | "5278901" | "5295230" | "5361359" | "5475625" | "5485409" | "5557742" | "5621889" | "5796942" | "5812763" | "5819094" | "5850516" | "5892903" | "5923849" | "5926463" | "5931946" | "5958010" | "5991881" | "6070244" | "6088804" | "6134664" | "6185689" | "6205552" | "6212558" | "6253337" | "6275942" | "6282546" | "6295607" | "6298445" | "6301613" | "6301668" | "6301699" | "6324656" | "6415321" | "6546493").PN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2019/05/01 16:40
S22	36	(user or adminstrator or operator) with (choos$4 or select$4 or pick$4 or designat$4) with firewall with (intrusion near2 (detect$4 or prevent$4) or ids or ips) and (intrusion near2 (detect$4 or prevent$4) or ids or ips) with (prevent$4 or thwart$4 or stop$4 or block$4 or inhibit$4 or prohibit$4) near5 connection	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/05/02 16:58
S23	270	(user or adminstrator or operator) with (choos$4 or select$4 or pick$4 or designat$4) with firewall with (intrusion near2 (detect$4 or prevent$4) or ids or ips)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/05/02 17:05
S24	153	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S23	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/05/02 17:27
L3	128	roll$2back$4 with (mitigat$4 or remediat$4 or firewall or intrusion near2 (detect$4 or prevent$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/05/03 12:09

EAST Search History (Interference)

< This search history is empty>

5/3/2019 5:40:37 PM
C:\Users\mherzog\Documents\EAST\Workspaces\App15608978.wsp

ForcePoint LLC
EX-1002
Page414

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
/M.R.H/	A	Action Summary for US Pat Appl No 14834102 dated 08/24/2918
/M.R.H/	B	Action Summary for US Pat Appl No 15608981 dated 11-05-2018
/M.R.H/	C	Action Summary for US Pat Appl No 15608983 dated 09-11-2018

/MADHURI R HERZOG/ 05/03/2019

Substitute Disclosure Form (PTO-1449)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	
Name/Print	Brian Owens	Registration Number	55517

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

ForcePoint LLC
EX-1002
Page416

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 2017-05-30	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: May 17, 2019

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

Additionally, related patent US8984644 is the subject of inter partes review (IPR No. IPR2017-02192), where Claims 1, 7, and 14 of such patent were held unpatentable.

ForcePoint LLC
EX-1002
Page417

Application No.: 15/608,978
Date: May 17, 2019
Information Disclosure Statement

This Information Disclosure Statement is being filed after the mailing date of a non-final Office Action. Accordingly, applicants are including payment in the amount of $120.00 for the fee due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-4964 (Order No. SP1P012C).

Respectfully submitted,



Dated: 17 May 2019

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page418

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P012C	Application No. 15/608,978
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Inventor Brett M. Oliphant	Confirmation Number 9647
		Filing Date 05/30/2017	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	A	Notice of Allowance for US Pat Appl No 15608983 dated 02-04-2019

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-05-17
Name/Print	Patrick Caldwell	Registration Number	44580

Electronic Patent Application Fee Transmittal	
Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C
Filed as Small Entity	
Filing Fees for Utility under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**120**

Electronic Acknowledgement Receipt	
EFS ID:	36050582
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	17-MAY-2019
Filing Date:	30-MAY-2017
Time Stamp:	21:26:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$120
RAM confirmation Number	052019INTEFSW21262800
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	SP1P012C_AmendmentC_vF_17-May-2019.pdf	103874 72956a13c2de581f16b7800bce6c65d032b1abd0	no	9
Warnings:					
Information:					
2	Transmittal Letter	SP1P012C_IDS_XMTL_vF_17-May-2019.pdf	55528 88790d4df16d4daa9e566c2188ad3138e703b6b5	no	2
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	SP1P012C_IDS_1449_vF_17-May-2019.pdf	55795 4b5d4ba834cd158591d8072ef2fd879064a1adc0	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Non Patent Literature	15608983.pdf	466923 cc539dd1df6e9b0c0c59ae6ccfd2797d86116dba	no	9
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30456 a62e61203173 9bfd5d06f63c730ecf96ea1efeed	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	712576		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: May 17, 2019

AMENDMENT C

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 05/08/19, please enter the following amendments

ForcePoint LLC
EX-1002
Page426

Remarks:

Claims 21-24 and 26-59 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more. Applicant respectfully disagrees with such rejection in view of the following.

Specifically, applicant respectfully notes that, in the recent USPTO "2019 Revised Patent Subject Matter Eligibility Guidance" ("Guidance"), the USPTO indicated, for Step 1 of the *Alice* test, that abstract ideas can be grouped as mathematical concepts, certain methods of organizing human activity, and mental processes. Importantly, claims that do not recite subject matter that falls within these enumerated groupings of abstract ideas should not be treated as reciting abstract ideas.

In the present application, one or more of the claims require "allow[ing] selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices" which clearly does not fall within the aforementioned groupings of abstract ideas.

In addition, applicant respectfully notes that, in the recent USPTO Guidance, the USPTO indicated, for Step 1 of the *Alice* test, that a patent application claim that recites a judicial exception is not ''directed to'' the judicial exception if the judicial exception is integrated into a practical application of the judicial exception. Further, examiners should evaluate integration into a practical application by: (a) identifying whether there are any additional elements recited in the claim beyond the judicial exception(s); and (b) evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application. In the context of the above, the following exemplary considerations are

C

ForcePoint LLC
EX-1002
Page427

indicative that an additional element (or combination of elements) may have integrated the exception into a practical application:

1) an additional element reflects an *improvement in the functioning of a computer*, or an *improvement to other technology or technical field*;

2) an additional element implements a judicial exception with, or uses a judicial exception in conjunction with, a *particular machine or manufacture* that is integral to the claim;

3) an additional element effects a *transformation or reduction of a particular article to a different state or thing*; and

4) an additional element applies or uses the judicial exception in some other meaningful way *beyond generally linking the use of the judicial exception to a particular technological environment*, such that the claim as a whole is more than a drafting effort designed to monopolize the exception.

Per the Guidance, this is not an exclusive list, and there may be other examples of integrating the exception into a practical application.

In the present application, even if the Examiner were to conclude that the claims fall within the aforementioned groupings of abstract ideas, the claims in the present application include one or more additional elements that extend beyond the judicial exception(s) and integrate the exception into a practical application. See the highlighted language below, just by way of example in the context of Claim 21, that represents an *improvement in the functioning of a computer* or *technical field* so as to *render the same* a *particular machine* (or method for operating the same) in a *particular technological environment.* See 1), 2) and 4) above.

C

ForcePoint LLC
EX-1002
Page428

"21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves **at least one operating system**." (emphasis added)

C

ForcePoint LLC
EX-1002
Page429

Finally, applicant respectfully notes that, in the recent USPTO Guidance, the USPTO indicated, for Step 2 of the *Alice* test, that if the Examiner concludes, under the Guidance, that an additional element is insignificant extra-solution activity, they should reevaluate that conclusion in Step 2 of the *Alice* test. If such reevaluation indicates that the element is *unconventional or otherwise more than what is well-understood, routine, conventional activity in the field*, this finding may indicate that an inventive concept is present and that the claim is thus eligible.

In the present case, even if the Examiner concludes that the above-highlighted elements are insignificant extra-solution activity, they are indeed unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, for at least the reason that the claim elements, individually and in combination, are not found in the prior art, as evidenced below by the fact that the Examiner's cited art is not even prior art.

Claims 21, 26 and 31 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Specifically, the Examiner argues that Claims 21, 26 and 31 recite the limitations: "first vulnerability information", "second vulnerability information", "accurately identified vulnerability" and "potential vulnerability". The use of the different terminology to indicate the various vulnerabilities has made the claims unclear. To improve the clarity of the claims, the examiner suggests using consistent language throughout the claims.

Applicant respectfully disagrees with this rejection. The claims specifically set forth the relationship between the "**first** vulnerability **information**", the "**second** vulnerability **information**", the "plurality of **potential vulnerabilities**", and/or the "at least one **accurately identified vulnerability**" (emphasis added). Just by way of example, Claim 21 states that the "second vulnerability **information** … is used to identify a plurality of **potential vulnerabilities**"

C

ForcePoint LLC
EX-1002
Page430

and the "**first** vulnerability **information** [is] generated utilizing the **second** vulnerability **information**, by: … determining that the plurality of devices is vulnerable to at least one **accurately identified vulnerability** (emphasis added), in the specific context claimed. Thus, it is clear from the claims as to the relationship between the relevant terms and, further, the claims clearly establish that the disputed terms are different claim elements with the aforementioned interrelationships that are clearly set forth in the claims. Since the claims clearly require different claim elements and establish the relationships therebetween, there is no "inconsistency" to be remedied.

Claims 21, 24, 26, 27, 31-33, 37, 38, 40, 41, 45, 46, 51 and 55-57 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7181769 to Keanini et al (hereinafter Keanini) and US 7509681 to Flowers et al (hereinafter Flowers). Applicant respectfully disagrees with this rejection.

Specifically, Applicant acknowledges that Keanini claims to be "a continuation-in-part of U.S. patent application Ser. No. 09/757,963 filed on Jan. 10, 2001 now U.S. Pat. No. 6,957,348, Ser. No. 09/757,872 filed on Jan. 10, 2001 and Ser. No. 09/648,211 filed on Aug. 25, 2000 now U.S. Pat. No. 7,073,198."

However, none of the above priority documents above disclose all of the subject matter in Keanini that is relied upon by the Examiner in attempting to meet applicant's claims, namely column 6, lines 54-67; column 7, lines 20-25, 49-67; column 10, lines 59-67; column 11, lines 15-25, 53-65; and column 12, lines 1-27.

Still yet, Applicant acknowledges that Keanini purportedly claims the benefit of "U.S. Provisional Application No. 60/388,078, filed on Jun. 11, 2002." First, the aforementioned provisional does not disclose all of the subject matter in Keanini that is relied upon by the Examiner in an attempt to meet applicant's claims, namely column 6, lines 54-67; column 7, lines 20-25, 49-67; column 10, lines 59-67; column 11, lines 15-25, 53-65; and column 12, lines 1-27.

C

ForcePoint LLC
EX-1002
Page431

Further, Keanini does not include a claim that is actually entitled to the benefit of priority of the provisional application. See the combination of terms highlighted from the independent claims from Keanini below:

> 1. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host, wherein a determined vulnerability pertains to a specific location and wherein the traffic monitor monitors for exploits of the determined vulnerability directed to the location and ignores exploits of the determined vulnerability directed to locations to which the determined vulnerability does not pertain. (emphasis added)

> 9. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host; and a centralized correlation server, communicatively coupled with the network at a centrally accessible

ForcePoint LLC
EX-1002
Page432

location, the device profiler and the traffic monitor, the centralized correlation server for receiving the determined vulnerabilities from the device profiler, identifying signatures of network traffic indicating attacks exploiting the determined vulnerabilities, and sending the signatures to the traffic monitor. (emphasis added)

16. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**, the device profiler including a low-level sensor for sending anomalous data packets to the host and determining the characteristics based on the host's response to the anomalous data packets; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host. (emphasis added)

Thus, Keanini is not proper prior art under *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375 (Fed. Cir. 2015), as a reference patent is only entitled to claim the benefit of the filing date of its provisional application if the disclosure of the provisional application provides support for the claims in the reference patent in compliance with § 112, ¶ 1. See MPEP 706.

In view of the above, Keanini can only rely on its June 6, 2003 filing date, which post-dates September 27, 2002, a date (but not necessarily the earliest date) as of which the claimed invention in the present application was conceived of and actually reduced to practice. Thus, Keanini is <u>not</u> prior art.

C

ForcePoint LLC
EX-1002
Page433

It is believed that all of the pending issues have been addressed. The claims are in condition for allowance. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, it should be noted that no claim is intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-4964 (Order No. SP1P012C).

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

Respectfully submitted,



Dated: 17 May 2019

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page434

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 07/23/2019

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER	
HERZOG, MADHURI R	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
07/23/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

Office Action Summary	**Application No.** 15/608,978	**Applicant(s)** Oliphant et al.	
	Examiner MADHURI R HERZOG	**Art Unit** 2438	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 05/17/2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 21-24 and 26-59 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 21-24 and 26-59 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 05/17/2019.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The following is a Final Office action in response to communications received 05/17/2019.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 05/17/2019 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

4. Claims 21-24 and 26-59 have been examined.

5. Examiner's rejection of the claims under 35 U.S.C 112 is withdrawn in light of the applicant's Remarks.

6. Applicant's arguments filed on 05/17/2019 with respect to the rejection under 35 U.S.C 101 have been fully considered but they are not persuasive. As per the applicant's arguments on pages 2-5 of the Remarks that the claims are eligible under 35 U.S.C 101, the examiner respectfully disagrees. Other than the recitation of one or more processors to perform the limitations, nothing in the claims limitations precludes the limitations from being performed in mind. For example, the limitations of receiving first vulnerability information that is generated from second vulnerability information,

ForcePoint LLC
EX-1002
Page437

generating first vulnerability information based on device configuration and second vulnerability information encompass a user manually identifying device configurations and generating first vulnerability information utilizing the device configurations and second vulnerability information. Similarly, the limitations of identifying an occurrence, determining that the vulnerability is susceptible to the occurrence and allowing selective utilization of mitigation actions encompass a user manually performing these limitations. Also, the processor is recited at a high-level of generality (*i.e.*, as a generic processor performing a generic computer function) such that it amounts no more than mere instructions to apply the exception using a generic computer component. Accordingly, this additional element does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea.

7. Applicant's arguments filed with respect to the rejection of claims 21, 24, 26, 27, 31-33, 37, 38, 40, 41, 45, 46, 51 and 55-57 under pre-AIA 35 U.S.C. 103(a) have been fully considered but they are not persuasive. As per the applicant's arguments that the prior art US 7181769 to Keanini et al is ineligible as prior art since there is no support for the subject matter cited in the previous office action from Keanini in the provisional application 60/338078 that Keanini has claimed priority to, the examiner respectfully disagrees. Applicant stated on page 6 of the Remarks that specifically, "column 6, lines 54-67; column 7, lines 20-25, 49-67; column 10, lines 59-67; column 11, lines 15-25, 53-65; and column 12, lines 1-27" of Keanini have no support in provisional application 60/338078. The examiner respectfully disagrees. US provisional application 60/338078 provides the following support to the cited subject matter:

ForcePoint LLC
EX-1002
Page438

a. **Column 6, lines 54-57 is supported by**: **Block on Exposure**: Page 4: 3.3: Network Address Translation; **IP360 Concepts Guide Paper**: pages 5-6, Sections 1.3-1.3.2; page 7, section 1.4.1.2; page 9: section 2: device profilers, page 9-10: section 2.1.1. **White Paper: Continuous Discovery as a Prerequisite for Security**: Page 7-8; **IP360 User Guide**: page 17, page 21-22.

b. **Column 7, lines 20-25, 49-67 is supported by**: **IP360 Concepts Guide Paper**: pages 5-6, Sections 1.3-1.3.2; page 7, section 1.4.1.2; page 9: section 2: device profilers, page 9-10: section 2.1.1; **White Paper: Continuous Discovery as a Prerequisite for Security**: Page 7-8; **White Paper: Monitoring Compliance to Manage Risk: Network Security Policy in Action**: page 8; **IP360 User Guide**: page 17, page 20-22.

c. **Column 10, lines 59-67 is supported by**: **IP360 Concepts Guide Paper**: page 7, section 1.4.1.2; **White Paper: Continuous Discovery as a Prerequisite for Security**: Page 7-8; **IP360 User Guide**: page 17.

d. **Column 11, lines 15-25, 53-65 is supported by**: **Block on Exposure**: Page 5, 4.2, 4th para; 4.2.1- block action taken; Page 7; page 8: 6.1: Action; **IP360 Concepts Guide Paper**: page 8, section 1.4.2.3; pages 10-11, section 2.2.

e. **Column 12, lines 1-27 is supported by**: **IP360 Concepts Guide Paper**: pages 5-6, Sections 1.3-1.3.2; page 7, section 1.4.1.2; page 9: section 2: device profilers, page 9-10: section 2.1.1; **White Paper: Continuous Discovery as a Prerequisite for Security**: Page 7-8; **White Paper: Monitoring Compliance to**

ForcePoint LLC
EX-1002
Page439

Manage Risk: Network Security Policy in Action: page 8; **IP360 User Guide**: page 17, page 21-22.

The documents cited above are present in the US provisional application 60/338078 in the order they have been cited.

Claim Rejections - 35 USC § 103

8. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 21, 24, 26, 27, 31-33, 37, 38, 40, 41, 45, 46, 51 and 55-57 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over prior arts of record US 7181769 to Keanini et al (hereinafter Keanini) and US 7509681 to Flowers et al (hereinafter Flowers).

As per claims 21 and 26, Keanini teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Keanini: column**

ForcePoint LLC
EX-1002
Page440

12, lines 1-27: The control module 320 identifies 1050 the total set of vulnerabilities for the host 191 from the vulnerability trees. Next, the control module 320 uses the sensors 345, 355 to verify 1060 the existence of the vulnerabilities on the host 191);

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Also, column 10, lines 59-67 and column 12, lines 1-27)**;

**ForcePoint LLC
EX-1002
Page441**

identify an occurrence in connection with at least one of the plurality of devices **(Keanini: column 11, lines 53-65: The traffic sniffing module 840 monitors network traffic to detect traffic corresponding to attack signatures in the attack signatures module 920. The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures);**

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information **(Keanini: column 11, lines 53-65: Preferably, the traffic sniffing module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic)**; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise**

ForcePoint LLC
EX-1002
Page442

network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs);

wherein the at least one configuration involves at least one operating system **(Keanini: column 7, lines 20-25: The low-level sensor 345 identifies operating systems running on hosts 191 and/or other characteristics)**.

Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach an intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

an intrusion prevention system-based occurrence mitigation type **(Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Flowers in the invention of Keanini to include an intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to not only allow an intrusion detection system (IDS) to leverage off the information gathered by the vulnerability detection system (VDS) but also allows a simple way to define rules for use by the vulnerability and intrusion detection systems to check for network conditions, such as vulnerabilities or intrusions (Flowers: column 2, lines 23-30).

As per claim 24, Keanini in view of Flowers teaches:

**ForcePoint LLC
EX-1002
Page443**

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Column 9, lines 35-67: The vulnerability tree for operating systems is similar to the application vulnerability tree 400 described above. For example, a top level of the tree can represent an operating system family (e.g., Unix, Windows, and MacOS) and descending levels can represent specific operating systems in each family (e.g., specific to Widows is XP, NT, 2000), operating system versions (e.g., specific to NT is 3.5 and 4.0), and patch levels (specific to 3.5 is Service Pack 1 and Service Pack 2). Also, column 10, lines 59-67 and column 12, lines 1-27).**

**ForcePoint LLC
EX-1002
Page444**

As per claim 31, Keanini teaches:

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities **(Keanini: column 12, lines 1-27: The control module 320 identifies 1050 the total set of vulnerabilities for the host 191 from the vulnerability trees. Next, the control module 320 uses the sensors 345, 355 to verify 1060 the existence of the vulnerabilities on the host 191)**;

said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191)**, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as**

"vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Also, column 10, lines 59-67 and column 12, lines 1-27);

display information that is based on the first vulnerability information **(Pearson: column 10, lines 3-23: The network profiling module 620 stores the information used by device profilers 165 to identify vulnerabilities and also stores the vulnerabilities of the system 100 detected by the device profilers 165. In one embodiment, the network profiling module 620 generates an abstract view of the configuration of the enterprise network 115 from the information collected from the individual device profilers 191)**;

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of**

a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs); and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices **(Keanini: column 11, lines 53-65: The traffic sniffing module 840 monitors network traffic to detect traffic corresponding to attack signatures in the attack signatures module 920. The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures)**;

wherein the at least one configuration involves at least one operating system **(Keanini: column 7, lines 20-25: The low-level sensor 345 identifies operating systems running on hosts 191 and/or other characteristics)**.

Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach an intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

an intrusion prevention system-based occurrence mitigation type **(Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Flowers in the invention of Keanini to include an intrusion prevention system-based occurrence mitigation type.

ForcePoint LLC
EX-1002
Page447

The motivation to do so would be to not only allow an intrusion detection system (IDS) to leverage off the information gathered by the vulnerability detection system (VDS) but also allows a simple way to define rules for use by the vulnerability and intrusion detection systems to check for network conditions, such as vulnerabilities or intrusions (Flowers: column 2, lines 23-30).

As per claims 27, 33 and 41, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence **(Keanini: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise**

ForcePoint LLC
EX-1002
Page448

network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs. Flowers: column 3, line 55-column 4, line 15: Thus, an IDS 116 used with an embodiment of the invention examines network traffic for signs of malicious activity. However, the rules loaded are determined by the VDS vulnerability analysis, so that only rules that describe possible intrusion conditions as they exist for the specific network 100 are loaded. So if a vulnerability V is identified, the intrusion detection system is target-based by virtue of the fact that it monitors the system running with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V).

As per claims 32 and 38, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence **(Keanini: column 11, lines 15-33: In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and**

ForcePoint LLC
EX-1002
Page449

alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64).

As per claim 37, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation **(Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

As per claim 40, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one accurately identified vulnerability **(Keanini: column 6, lines 54-67: In operation, the control module 320 identifies hosts 191 on the network and characteristics of the hosts 191 and use the characteristics to determine the host's vulnerabilities. Column 7, lines 49-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred**

ForcePoint LLC
EX-1002
Page450

to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. Column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs).

As per claim 45, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: determine the occurrence to have a first severity if it is determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence; determine the occurrence to have a second severity if it determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is not susceptible to

ForcePoint LLC
EX-1002
Page451

being taken advantage of by the occurrence; and report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity **(Keanini: column 2, lines 55-67: A traffic monitor monitors network traffic for attack signatures corresponding to the determined vulnerabilities to detect malicious activity. In one embodiment, the traffic monitor associates attack signatures with the specific destination (e.g., IP address and/or port) having the corresponding vulnerability. The traffic monitor does not signal an attack unless the attack matches the attack signature of an exploit of a vulnerability and is directed to a destination known to have the vulnerability. Column 11, lines 53-65: Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Additionally, the traffic sniffing module 930 is configured to send a notification message to the centralized correlation server 175 in response to detecting an attack signature. Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked)**.

As per claim 46, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence

ForcePoint LLC
EX-1002
Page452

mitigation action of the intrusion prevention system-based occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action **(Keanini: Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked. In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Column 2, lines 43-62: The rules used by the VDS and IDS are easily formed and therefore, an end user, such as a security or network engineer, can easily define and construct rules beyond any that are defined by the VDS/IDS provider)**.

As per claim 51, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to: based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one accurately identified vulnerability while there is no installation of a patch that removes the at least one accurately identified vulnerability **(Keanini: Column 12, lines 52-67: In one embodiment, the notification is sent to block vulnerabilities that have a high probability of being attacked, or that have a high consequence as a result of being attacked. In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the**

ForcePoint LLC
EX-1002
Page453

centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Column 2, lines 43-62: The rules used by the VDS and IDS are easily formed and therefore, an end user, such as a security or network engineer, can easily define and construct rules beyond any that are defined by the VDS/IDS provider).

As per claim 55, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused **(Keanini: column 2, lines 29-37: The control module determines a set of potential vulnerabilities by summing the vulnerabilities at each traversed node. The control module determines whether the vulnerabilities actually exist on the host and sends a list of the verified vulnerabilities to the centralized correlation server. Column 11, lines 53-65: The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures. Preferably, the traffic sniffing module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic. Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Column 12, lines 52-67: In response to receiving 1210 a notification related to vulnerabilities sent by the device profiler 165, the event**

ForcePoint LLC
EX-1002
Page454

daemon module 820 performs a set of actions such as configuring 1220 the firewall 150 to prevent the attack).

As per claim 56, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence **(Keanini: Column 11, lines 53-65: The traffic sniffing module 840 analyzes network traffic to identify patterns matching the attack signatures. Preferably, the traffic sniffing module 840 uses the subsets of attack signatures to monitor for only exploits of vulnerabilities present at the destination of the traffic. Thus, the traffic sniffing module 840 will ignore an attack signature directed to a destination (e.g., IP address and/or port) that is not vulnerable to the exploit. Column 12, lines 52-67: In response to receiving 1210 a notification related to vulnerabilities sent by the device profiler 165, the event daemon module 820 performs a set of actions such as configuring 1220 the firewall 150 to prevent the attack)**.

As per claim 57 Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the

occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system- based occurrence mitigation type being selectively caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence **(Keanini: column 11, lines 15-33: In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64)**.

11. Claims 22, 23, 28-30, 34-36, 39, 42, 44, 47-50, 52-54, 58 and 59 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Keanini in view of Flowers as applied to claim 21, 26 and 31 above, and further in view of US 20050235360 to Sterling Michael Pearson (hereinafter Pearson).

As per claim 22, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least

ForcePoint LLC
EX-1002
Page456

one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device. However, Pearson teaches:

wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a

ForcePoint LLC
EX-1002
Page457

second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for

ForcePoint LLC
EX-1002
Page458

preventing at least one occurrence packet, and an intrusion prevention- type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 23, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured such that at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence

ForcePoint LLC
EX-1002
Page459

packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device. However, Flowers teaches:

wherein the instructions are configured such that at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area**

ForcePoint LLC
EX-1002
Page460

325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that at least two options are provided including a firewall- type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 28, 34 and 58, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence

ForcePoint LLC
EX-1002
Page461

mitigation type but does not explicitly teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area**

ForcePoint LLC
EX-1002
Page462

325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions, when executed by the one or more processors, cause the one or more processors to: receive a first user input; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 29 and 35, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a

ForcePoint LLC
EX-1002
Page463

manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence. However, Flowers teaches:

wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out**

ForcePoint LLC
EX-1002
Page464

predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input is results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence. The motivation

ForcePoint LLC
EX-1002
Page465

to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 30 and 36, Keanini in view of Flowers teaches a firewall-based occurrence mitigation type and intrusion prevention system-based occurrence mitigation type but does not explicitly teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Flowers teaches:

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface;

ForcePoint LLC
EX-1002
Page466

and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one

ForcePoint LLC
EX-1002
Page467

user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 39, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only relevant occurrence mitigation actions are available for selection by the user **(Flowers: column 4, lines 1-15: Such a Target-based IDS will have the ability to monitor for specific conditions to which the network has been determined to be vulnerable, as well as any range of conditions or attacks to which the network might be vulnerable. For instance, if the VDS finds a type of service S, but has not verified S's vulnerability to a buffer overflow condition, the IDS may still monitor for such a buffer overflow. So if a vulnerability V is identified, the intrusion detection system is target-based by virtue of the fact that it monitors the system running**

ForcePoint LLC
EX-1002
Page468

with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V).

Keanini in view of Flowers does not explicitly teach: one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user. However, Pearson teaches:

one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include one or more options are provided to a user and only relevant occurrence mitigation actions are available for selection by the user. The motivation to do so would be to remotely configure and monitor a communication

ForcePoint LLC
EX-1002
Page469

device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 42, Keanini in view of Flowers teaches reporting of the occurrence but does not explicitly teach: wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device. However, Pearson teaches:

wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to**

ForcePoint LLC
EX-1002
Page470

certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 44, Keanini in view of Flowers does not teach: wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the

ForcePoint LLC
EX-1002
Page471

different occurrence mitigation actions are associated with the single actual vulnerability. However, Pearson teaches:

wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types

ForcePoint LLC
EX-1002
Page472

in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 47, Keanini in view of Flowers does not teach: wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options. However, Pearson teaches:

wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a

ForcePoint LLC
EX-1002
Page473

first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded)**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed

ForcePoint LLC
EX-1002
Page474

via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 48, Keanini in view of Flowers does not teach: wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. However, Pearson teaches:

ForcePoint LLC
EX-1002
Page475

wherein the instructions, when executed by the one or more processors, cause the one or more processors to: display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a**

ForcePoint LLC
EX-1002
Page476

conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface; receive a first user input selecting a first one of the options, utilizing the at least one user interface; based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; receive a second user input selecting a second one of the options, utilizing the at least one user interface; and based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 49, Keanini in view of Flowers and Pearson teaches:

The non-transitory computer-readable media of Claim 48, wherein the instructions are configured such that the automatic application of the first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type includes

ForcePoint LLC
EX-1002
Page477

sending a second signal to at least one component with intrusion prevention system functionality **(Keanini: column 12, lines 52-67: In response to receiving 1230 notification of malicious activity from a traffic monitor 185, the centralized correlation server 175 performs a set of actions such as configuring the firewall 150 in real-time to block the attack. Flowers: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-67 and column 4, lines 1-15: So if a vulnerability V is identified, the intrusion detection system is target-based by virtue of the fact that it monitors the system running with vulnerability V, it monitors for attacks on V, and it monitors for attacks that make sense to look for given the presence of V)**.

As per claim 50, Keanini in view of Flowers does not teach: wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences. However, Pearson teaches:

wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the

ForcePoint LLC
EX-1002
Page478

identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences (**Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. [0065] Preferably, the advanced options information display area 325 provides a selectable option or intrusion rule for each listed attack so that the user may configure the communication device 106 to monitor selected types of communications and to establish a security level or policy for each. [0049]: Accordingly, in the disclosed embodiment the firewall 162 may be of a conventional type, used in the known manner, for shielding the LAN 104 from communications traffic determined by the firewall to be excluded**).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are

ForcePoint LLC
EX-1002
Page479

automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 52, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device **(Keanini: column 11, lines 53-65)**; the determining that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine whether a first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet **(Keanini: column 11, lines 53-65. Flowers: column 3, line 55-column 4, line 15)**, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least

ForcePoint LLC
EX-1002
Page480

one second occurrence packet **(Keanini: column 11, lines 53-65. Flowers: column 3, line 55-column 4, line 15)**; and the allowing the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface **(Keanini: column 11, lines 15-25 and column 10, lines 3-10. Flowers: column 2, lines 42-47)**; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed by sending a first signal over at least one network to a first component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device **(Keanini: column 12, lines 52-67)**; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type is completed by sending a second signal to a second component with an intrusion prevention system type functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device **(Flowers: column 3, line 55-column 4, line 15)**.

Keanini in view of Flowers does not explicitly teach based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed. However, Pearson teaches:

based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is

ForcePoint LLC
EX-1002
Page481

completed **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall- based occurrence mitigation type is completed. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claim 53, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 52, wherein the instructions are configured such that at least one of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Keanini: column 5, lines 26-33)**; said second vulnerability

ForcePoint LLC
EX-1002
Page482

information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith **(Keanini: column 12, lines 40-52)**; said first vulnerability information is generated via a vulnerability scan operation **(Keanini: column 7, lines 1-7)**; said first device, said second device, and said third device are part of the same group **(Keanini: column 4, lines 5-25)**; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status **(Keanini: column 10, lines 5-10)**; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration is identified via user input in connection with at least one setting **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability **(Keanini: column 12, lines 52-67)**; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Keanini: column 12, lines 52-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Flowers: Abstract, column 3, line 55-column 4, line 15)**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of

devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different

ForcePoint LLC
EX-1002
Page484

occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said at least one accurately identified vulnerability includes the at least one operating system **(Keanini: column 9, lines 45-65)**; said actual vulnerabilities include the at least one accurately identified vulnerability **(Keanini: column 2, lines 4-16)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which includes the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types; said different occurrence mitigation actions include different remediation actions **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation

ForcePoint LLC
EX-1002
Page485

actions **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Keanini: column 11, lines 43-65)**; said at least one aspect of the at least one first occurrence packet involves at least one of a payload thereof or an IP address **(Keanini: column 11, lines 43-65)**; said at least one aspect of the at least one first occurrence packet is utilized to determine whether the first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, by utilizing the at least one aspect in connection with at least one of a cross-referencing operation or a look-up operation **(Keanini: column 11, lines 43-65)**; said first signal and the second signal include at least one of response signals, or signals sent in response to a query signal **(Keanini: column 11, lines 43-65 and column 12, lines 52-67)**; said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality **(Keanini: column 12, lines 52-67)**; said second component with the intrusion prevention system type functionality includes at least one of an intrusion prevention system, an intrusion detection system with the intrusion prevention system type functionality, a gateway with the intrusion prevention system type functionality, a router with the intrusion prevention system type functionality, a sensor with the intrusion prevention system type functionality, or a multiple-security product system with the intrusion prevention system type functionality **(Flowers: column 3, lines 55-67)**; said preventing includes at least one of rejecting a

request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or said automatic response includes a real-time response **(Keanini: column 12, lines 52-67)**.

Keanini in view of Flowers does not teach: said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. However, Pearson teaches:

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action. The motivation to do so would be to remotely configure and monitor a

ForcePoint LLC
EX-1002
Page487

communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

As per claims 54 and 59, Keanini in view of Flowers teaches:

The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of: said at least one first data storage includes at least one first database; said at least one second data storage includes at least one second database **(Keanini: column 5, lines 26-33)**; said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith **(Keanini: column 12, lines 40-52)**; said first vulnerability information is generated via a vulnerability scan operation **(Keanini: column 7, lines 1-7)**; said first vulnerability information identifies at least one actual vulnerability **(Keanini: column 2, lines 4-16)**; said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities **(Keanini: column 5, lines 25-40)**; said first device, said second device, and said third device are part of the same group **(Keanini: column 4, lines 5-25)**; said at least one configuration includes at least one of configuration data, configuration information, or a configuration status **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration includes at least one of a configuration option, a policy setting, or a patch **(Keanini: column 10, lines 5-10. Flowers: column 2, lines 43-47)**; said at least one configuration is utilized for identifying the at least one operating system or an application **(Keanini: column 7,**

ForcePoint LLC
EX-1002
Page488

lines 20-25); said at least one configuration is identified utilizing information regarding the at least one operating system or an application **(Keanini: column 7, lines 20-25)**; said at least one configuration is identified via user input in connection with at least one setting **(Keanini: column 10, lines 5-10)**; said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability; said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall **(Keanini: column 12, lines 52-67)**; said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system **(Flowers: Abstract, column 3, line 55-column 4, line 15)**; said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the

ForcePoint LLC
EX-1002
Page489

different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices **(Keanini: column 11, lines 15-25 and column 12, lines 52-67)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability **(Keanini: column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said at least one actual vulnerability is the at least one operating system **(Keanini: column 9, lines 45-65)**; said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at

ForcePoint LLC
EX-1002
Page490

least one operating system **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said different occurrence mitigation actions include different remediation actions; said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions **(Keanini: column 9, lines 45-65, column 11, lines 15-25, 53-65 and column 12, lines 52-67. Flowers: Abstract)**; said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack **(Keanini: column 11, lines 43-65)**; said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration **(Keanini: column 2, lines 29-37, column 20-65)**; said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software **(Keanini: column 7, lines 8-46)**; said determining that the plurality of devices is actually vulnerable to the at

ForcePoint LLC
EX-1002
Page491

least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration **(Keanini: column 7, lines 49-67 and column 8, lines 27-56)**; said non-transitory computer-readable media includes a single non-transitory computer readable medium; one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time; one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation **(Keanini: column 12, lines 52-67. Flowers: column 3, lines 55-67)**; one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch **(Flowers: column 3, lines 55-67)**; one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component **(Keanini: column 12, lines 52-67)**; and wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation **(Keanini: column 12, lines 52-67)**, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices **(Keanini: column 7, lines 8-46)**.

Keanini in view of Flower does not explicitly teach: one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; and to deploy a patch. However, Pearson teaches:

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time **(Pearson: [0063] The user may easily configure the security policy for communication device 106 by selecting one of the radio buttons, and then clicking the submit button 224. As will be described in more detail below with reference to FIG. 11, the user-selected security level is utilized to configure the firewall and intrusion detection features of communication device 106 in accordance with the user's preferences, to carry out predetermined responses to certain predetermined threats. For example, a high security level may be a policy that monitors for any type of file transfer protocol (ftp) communication received from any source, and responds to such ftp communication by terminating the communication. Also, [0065], [0049])**;

to deploy a patch **(Pearson: Based upon the received status information, the remote computer then determines whether the communication device requires a software update. If the device requires such a software update, the remote computer queues any necessary software patches for later download to the communication device. Also, [0044])**.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Pearson in the invention of Keanini in view of Flowers to include one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time; and to deploy a patch. The motivation to do so would be to remotely configure and monitor a communication device, for example a firewall, an intrusion detection device, or similar Internet appliance (Pearson: [0008]).

ForcePoint LLC
EX-1002
Page493

12. Claim 43 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Keanini in view of Flowers as applied to claim 41 above, and further in view of prior art of record US 20030126472 to Carl Banzhof (hereinafter Banzhof).

As per claim 43, Keanini in view of Flowers does not teach: wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. However, Banzhof teaches:

wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device (Banzhof: [0031]: In box 86, the client user, typically an IT person or other computer security personnel, is given the opportunity to select which vulnerabilities should be remediated. Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability does not pose a sufficient security risk, the remediation signature is deemed too risky, etc. [0032]: If the remediation is not deemed

ForcePoint LLC
EX-1002
Page494

successful, either because it did not resolve the identified vulnerabilities as evidenced by an additional security scan of the client computer, or because the remediation actions had unintended deleterious effects, etc., then the remediation can be rolled back or undone and the remediation process can be repeated as indicated in box 99).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Banzhof in the invention of Keanini in view of Flowers to include wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device. The motivation to do so would be to provide for a more automated and managed way to remediate security vulnerabilities on individual computers and computer networks (Banzhof: [0007]).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 20030204632 to Willebeek-LeMair et al: A network discovery functionality, intrusion detector functionality and firewalling functionality are integrated together to form a network security system presenting a self-deploying and self-hardening security defense for a network.

ForcePoint LLC
EX-1002
Page495

US 20070011319 to McClure et al: A system and method provide comprehensive and highly automated testing of vulnerabilities to intrusion on a target network, including identification of operating system, identification of target network topology and target computers, identification of open target ports, assessment of vulnerabilities on target ports, active assessment of vulnerabilities based on information acquired from target computers, quantitative assessment of target network security and vulnerability, and hierarchical graphical representation of the target network, target computers, and vulnerabilities in a test report.

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI R HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on 8:30AM-5:00PM.

ForcePoint LLC
EX-1002
Page496

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MADHURI R. HERZOG
Primary Examiner
Art Unit 2438

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1002
Page497

Notice of References Cited	Application/Control No. 15/608,978	Applicant(s)/Patent Under Reexamination Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030204632-A1	10-2003	Willebeek-LeMair, Marc	H04L29/06	709/249
*	B	US-20070011319-A1	01-2007	McClure; Stuart C.	G02B6/105	709/224
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019	07/18/2019					
	1	-	-	-	-					
	2	-	-	-	-					
	3	-	-	-	-					
	4	-	-	-	-					
	5	-	-	-	-					
	6	-	-	-	-					
	7	-	-	-	-					
	8	-	-	-	-					
	9	-	-	-	-					
	10	-	-	-	-					
	11	-	-	-	-					
	12	-	-	-	-					
	13	-	-	-	-					
	14	-	-	-	-					
	15	-	-	-	-					
	16	-	-	-	-					
	17	-	-	-	-					
	18	-	-	-	-					
	19	-	-	-	-					
	20	-	-	-	-					
	21	✓	✓	✓	✓					
	22	✓	✓	✓	✓					
	23	✓	✓	✓	✓					
	24	✓	✓	✓	✓					
	25	✓	-	-	-					
	26	✓	✓	✓	✓					
	27	✓	✓	✓	✓					
	28	✓	✓	✓	✓					
	29	✓	✓	✓	✓					
	30	✓	✓	✓	✓					
	31	✓	✓	✓	✓					
	32	✓	✓	✓	✓					
	33	✓	✓	✓	✓					
	34	✓	✓	✓	✓					
	35	✓	✓	✓	✓					
	36	✓	✓	✓	✓					
	37	✓	✓	✓	✓					
	38		✓	✓	✓					
	39		✓	✓	✓					
	40		✓	✓	✓					
	41		✓	✓	✓					
	42		✓	✓	✓					

ForcePoint LLC
EX-1002
Page499

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019	07/18/2019					
	43		✓	✓	✓					
	44		✓	✓	✓					
	45		✓	✓	✓					
	46		✓	✓	✓					
	47		✓	✓	✓					
	48		✓	✓	✓					
	49		✓	✓	✓					
	50		✓	✓	✓					
	51		✓	✓	✓					
	52		✓	✓	✓					
	53		✓	✓	✓					
	54		✓	✓	✓					
	55		✓	✓	✓					
	56		✓	✓	✓					
	57		✓	✓	✓					
	58		✓	✓	✓					
	59		✓	✓	✓					

ForcePoint LLC
EX-1002
Page500

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

CPC - Searched*		
Symbol	Date	Examiner
H04L 63/02$, 63/14$, 63/20$	07/18/2019	M.H
G06F 21/5$	07/18/2019	M.H

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search, Assignee search	07/18/2019	M.H
East search	07/18/2019	M.H

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page501

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	A	Notice of Allowance for US Pat Appl No 15608983 dated 02-04-2019

/MADHURI R HERZOG/ 07/18/2019

Substitute Disclosure Form (PTO-1449)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

ForcePoint LLC
EX-1002
Page502

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-05-17
Name/Print	Patrick Caldwell	Registration Number	44580

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

ForcePoint LLC
EX-1002
Page503

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S26	2018	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or examin$6 or analy$4 or scan$4 or prob$4) with (host or client or device or machine or equipment) with (operating near2 system or os) and (determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or examin$6 or analy$4 or scan$4 or prob$4) with (host or client or device or machine or equipment) with (vulnerabilit$4 or exploit$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/07/17 15:32
S27	1399	(vulnerabilit$4 or exploit$4) with (specific or pertinent or applicable or relevan$4 or characteristic or typical$3 or representative) with (operating system or os or (device or host or node or terminal or equipment or machine) near5 (profile or configuration))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/07/17 15:38
S29	305	S26 and S27	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/07/17 15:39
S30	279	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S29	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/07/17 15:40
S31	286	S29 and (firewall or ids or intrusion$4detection$4system or ips or intrusion$4prevention$4system)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/07/17 16:01

EAST Search History (Interference)

< This search history is empty>

7/18/2019 9:23:54 AM
C:\Users\mherzog\Documents\EAST\Workspaces\App15608978.wsp

ForcePoint LLC
EX-1002
Page504

Electronic Acknowledgement Receipt	
EFS ID:	36707014
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	26-JUL-2019
Filing Date:	30-MAY-2017
Time Stamp:	23:33:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response After Final Action	SP1P012C_AmendmentD_vF_26-Jul-2019.pdf	104118 e2bbc47887d3a03d5f8e4291dc48ecf8b4cdc01b	no	8

Warnings:

Information:	
Total Files Size (in bytes):	104118

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: July 26, 2019

AMENDMENT D

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 07/23/19, please enter the following:

C

ForcePoint LLC
EX-1002
Page507

Remarks:

Claims 21-24 and 26-59 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more. Specifically, in the latest Office Action mailed 7/23/2019, the Examiner argues that "[o]ther than the recitation of one or more processors to perform the limitations, nothing in the claims limitations precludes the limitations from being performed in mind." Applicant respectfully disagrees.

Argument #1

First, with respect to Claim 21, for example, the following emphasized claim terms can NOT be performed in mind:

> "**identify an occurrence in connection with at least one of the plurality of devices;**
> **determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information**; and
> allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for **occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices**" (emphasis added).

Clearly, a person's "mind" cannot: determine that at least one accurately identified vulnerability is susceptible to being taken advantage of by an occurrence identified, utilizing the first vulnerability information; and prevent advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across devices, in the specific context claimed.

In a similar context in *SRI International, Inc. v. Cisco Systems, Inc*. (Fed. Cir. 2019), the Federal Circuit confirmed the District Court's Step One determination that "claim 1 is not directed to an abstract idea" because the "claims are directed to using a specific technique—using a plurality

C

ForcePoint LLC
EX-1002
Page508

of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: **identifying hackers or potential intruders into the network**" (emphasis added).

In explanation, the Federal Circuit opinion states:

> "…the claims here are not directed to using a computer as a tool—that is, automating a conventional idea on a computer. Rather, the representative claim improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security.
>
> Indeed, **we tend to agree with [Plaintiff] that the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets** ..." (emphasis added).

Thus, similar to *SRI International*, the current claims recite security-related activity that simply cannot be performed by the human mind, and, thus, the current claims are not directed to an abstract idea.

Argument #2

Second, it appears the Examiner *did not even address* applicant's arguments with respect to Step 2 of the *Alice* test.

Specifically, in the present application, even if the Examiner were to conclude that the claims fall within the appropriate groupings of abstract ideas, the claims in the present application include one or more additional elements that extend beyond the judicial exception(s) and integrate the exception into a practical application. See the highlighted language below, just by way of example in the context of Claim 21, that represents an *improvement in the functioning of a computer* or *technical field* so as to *render the same* a *particular machine* (or method for operating the same) in a *particular technological environment.*

> "21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

ForcePoint LLC
EX-1002
Page509

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves **at least one operating system**." (emphasis added)

Further, applicant respectfully notes that, in the recent USPTO Guidance, the USPTO indicated, for Step 2 of the *Alice* test, that if the Examiner concludes, under the Guidance, that an additional element is insignificant extra-solution activity, they should reevaluate that conclusion in Step 2 of the *Alice* test. If such reevaluation indicates that the element is *unconventional or otherwise more than what is well-understood, routine, conventional activity in the field*, this finding may indicate that an inventive concept is present and that the claim is thus eligible.

In the present case, even if the Examiner concludes that the above-highlighted elements are insignificant extra-solution activity, they are indeed unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, for at least the reason that the claim elements, individually and in combination, are not found in the prior art. Further, as evidenced below, the Examiner's cited art is <u>not</u> even prior art.

C

ForcePoint LLC
EX-1002
Page510

Claims 21, 24, 26, 27, 31-33, 37, 38, 40, 41, 45, 46, 51 and 55-57 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7181769 to Keanini et al (hereinafter Keanini) and US 7509681 to Flowers et al (hereinafter Flowers). Specifically, in the latest Office Action mailed 7/23/2019, the Examiner argues that "US provisional application 60/338078 provides … support to the cited subject matter." Applicant respectfully disagrees.

Argument #1

In particular, with respect to Claim 21, the Examiner appears to rely on "Block on Exposure: Page 5, 4.2, 4th para; 4.2.1- block action taken; Page 7; page 8: 6.1: Action; IP360 Concepts Guide Paper: page 8, section 1.4.2.3; pages 10-11, section 2.2." to make a prior art showing of applicant's claimed technique to "allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices."

In doing so, the Examiner admits that "Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach an intrusion prevention system-based occurrence mitigation type." However, simply disclosing a firewall in the forgoing Keanini excerpts does not meet applicant's claimed technique to "**allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types**, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities **utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices**," in the specific context claimed (emphasis added).

C

ForcePoint LLC
EX-1002
Page511

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. With respect to the other independent claims, applicant respectfully asserts that such claims are deemed allowable for reasons similar, but not necessarily identical, to one or more of the aforementioned reasons (see each claim for specific claim language contained therein).

Argument #2

Second, it appears the Examiner *did not even address* applicant's arguments that Keanini does not include a claim that is actually entitled to the benefit of priority of the provisional application. See the combination of terms highlighted from the independent claims from Keanini below:

> 1. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host, wherein a determined vulnerability pertains to a specific location and wherein the traffic monitor monitors for exploits of the determined vulnerability directed to the location and

C

ForcePoint LLC
EX-1002
Page512

ignores exploits of the determined vulnerability directed to locations to which the determined vulnerability does not pertain. (emphasis added)

9. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host; and a centralized correlation server, communicatively coupled with the network at a centrally accessible location, the device profiler and the traffic monitor, the centralized correlation server for receiving the determined vulnerabilities from the device profiler, identifying signatures of network traffic indicating attacks exploiting the determined vulnerabilities, and sending the signatures to the traffic monitor. (emphasis added)

16. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**, the device profiler including a low-level sensor for sending anomalous data packets to the host and determining the characteristics based on the host's response to the anomalous data packets; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host. (emphasis added)

Thus, Keanini is not proper prior art under *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375 (Fed. Cir. 2015), as a reference patent is only entitled to claim the benefit of the filing date of its provisional application if the disclosure of the provisional application provides support for the claims in the reference patent in compliance with § 112, ¶ 1. See MPEP 706.

In view of the above, Keanini can only rely on its June 6, 2003 filing date, which post-dates September 27, 2002, a date (but not necessarily the earliest date) as of which the claimed invention in the present application was conceived of and actually reduced to practice. Thus, Keanini is <u>not</u> prior art.

ForcePoint LLC
EX-1002
Page513

It is believed that all of the pending issues have been addressed. The claims are in condition for allowance. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, it should be noted that no claim is intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-4964 (Order No. SP1P012C).

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

Respectfully submitted,



Dated: 26 Jul 2019

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page514

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 08/13/2019

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER	
HERZOG, MADHURI R	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
08/13/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 15/608,978	**Applicant(s)** Oliphant et al.	
	Examiner MADHURI R HERZOG	**Art Unit** 2438	**AIA (FITF) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 July 2019 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☑ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires ____ months from the mailing date of the final rejection.
   b) ☑ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection.The current period for reply expires ____ months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.
   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANTS FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____ (See 37CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicants reply has overcome the following rejection(s): _____
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☑ For purposes of appeal, the proposed amendment(s):(a) ☐ will not be entered, or (b) ☑ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☑ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☐ Other: _____.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
    Claim(s) allowed:_____.
    Claim(s) objected to:_____.
    Claim(s) rejected:21-24 and 26-59.
    Claim(s) withdrawn from consideration:_____.

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

C

ForcePoint LLC
EX-1002
Page516

Continuation of REQUEST FOR RECONSIDERATION/OTHER 12. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: As per the applicant's argument #1 under 35 U.S.C 101 rejection that the highlighted claim limitations cannot be performed in the mind, the examiner respectfully disagrees. The applicant cites SRI International, Inc. v. Cisco Systems, Inc. (Fed. Cir. 2019). However, unlike the cited case, the highlighted limitations of the claims in the instant application do not recite network monitors or analyzing network packets. The limitation: "identify an occurrence in connection with at least one of the plurality of devices" does not specify the type of occurrence. One of ordinary skill in the art can broadly interpret the occurrence to be any occurrence that is easily identifiable with the human mind including malfunction of a device. Similarly, the limitation: "determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information" is easily performed manually by a human by correlating the occurrence with the list of vulnerabilities that the device under consideration has. Similarly, the limitation: "allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices" is also easily performed manually by a human by selecting manually a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type to prevent a vulnerability of a device from being used by the occurrence. For example, when a device is deemed susceptible, a person can manually activate a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type to prevent the device from being taken advantage of. Regarding applicant's argument # 2 that the claims are eligible under step 2, the examiner respectfully disagrees. The claims do not recite any additional elements other than a processor at a high level of generality. The use of the processor at a high level of generality amounts to no more than mere instructions being applied to the exception using a generic computer component. Also, the applicant indicates that the claims elements, individually or in combination, are not found in prior art with which the examiner respectfully disagrees. Prior art Keanini is a prior art as will be shown below.
Regarding the rejection under 35 U.S.C 103, per argument #1, prior art of record Keanini does not teach the limitation: "allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types…", the examiner respectfully disagrees. Keanini teaches: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191 , and/or preventing the operating systems and/or applications from executing programs (different occurrence mitigation actions of diverse occurrence mitigation types). Keanini teaches allowing selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types including the firewall mitigation type. As indicated in the previous office actions, the diverse mitigation types used by Keanini do not explicitly recite an intrusion prevention system-based occurrence mitigation type. Prior art of record Flowers teaches: Abstract: The intrusion detection system leverages off of information gathered about a network, such as vulnerabilities, so that it only examines and alerts the user to potential intrusions that could actually affect the particular network. Also, column 3, lines 42-64. Regarding Argument #2, it is unclear why Keanini's claims are under scrutiny when support for the subject matter cited in rejecting the claims has been shown to be present in the provisional application 60/388078. Regardless, regarding the applicant's arguments that the highlighted terms: "according to a tree-structured vulnerability table" are not supported, the examiner respectfully disagrees. According to Keanini, column 7, lines 50-67: In one embodiment, the rules database module 365 also stores potential vulnerabilities of hosts in one or more tree-like data structures, referred to as "vulnerability trees" 400 (e.g., an application vulnerability tree and an operating system vulnerability tree). The control module 320 is adapted to fire rules in the rules

database module 365 that use the high-355 and/or low-level sensors 345 to determine the host's characteristics and use these characteristics to traverse the vulnerability tree 400 and identify potential vulnerabilities at each host 191. In one embodiment, the rules database module 365 also stores rules to verify the potential vulnerabilities. The rules database module 365 is preferably configured to receive occasional rule updates from the centralized correlation server 175. This is supported in the provisional application: IP360 Concepts Guide, page 9, section 2.1: The IP360 network discovery process operates on Device Profiler appliances installed at strategic points throughout a network. During the discovery process, the network is continuously probed for exposures. During the discovery process, IP360 investigates: • Externally exposed IP network devices, such as web servers, mail servers and FTP servers • Internal IP network devices • All inactive IP addresses to verify that only authorized devices are attached to the network From these exposures, IP360 identifies the operating systems and applications on each active IP device. It evaluates the exposures relative to known vulnerabilities and corporate security policies, and highlights areas of non-compliance. For example, if the enterprise has a policy that no mail servers are to be run on Linux, and a Linux mail server is discovered, that security policy violation can be investigated and corrected. Section 2.1.1: After the OS is discovered, each device is individually explored to find the applications running on the device. The Device Profiler uses conditional rules to determine which probes are relevant to send to each host. The data captured from these repeated discovery sessions creates a history of each IP device's exposures, from which reports are produced. Continuous Discovery as a Prerequisite for Security, page 7: Overview of IP360 functionality. IP360 Device Profiler appliances collect the exposures of the device on each IP address, and from that information, they determine the characteristics (i.e., operating system, applications) of the device. From the exposures, the Device Profilers generate a list of vulnerabilities to which the device is susceptible. Page 8: Vulnerabilities Database. After the reflex tests are completed, IP360 compares the exposures identified on each device to the database of known vulnerabilities, then creates device-specific list of vulnerabilities that is used by the Traffic Monitors. IP360 uses conditional rules to efficiently search the vulnerabilities database. For example, on a scan where the detected operating system is Solaris, the Device Profiler does not check for the ida/idq mapping vulnerability, because that vulnerability only exists on Windows NT.

ForcePoint LLC
EX-1002
Page518

OK TO ENTER: /M.R.H/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: July 26, 2019

AMENDMENT D

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 07/23/19, please enter the following:

C

ForcePoint LLC
EX-1002
Page519

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15/608,978	Filing Date	2017-05-30	Docket Number (if applicable)	SP1P012C	Art Unit	2438
First Named Inventor	Brett M. Oliphant			Examiner Name	Madhuri R HERZOG		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 505939

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-09-03
Name	Patrick Caldwell	Registration Number	44580

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	31	50	1550
INDEPENDENT CLAIMS IN EXCESS OF 3	2201	1	230	230
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	2820	1	950	950
		Total in USD ($)		**2730**

Electronic Acknowledgement Receipt	
EFS ID:	37056297
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	03-SEP-2019
Filing Date:	30-MAY-2017
Time Stamp:	23:07:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2730
RAM confirmation Number	E201993N07253340
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SP1P012C_RCE_vF_03-Sep-2019.pdf	1364038 443d579cc414bf631b0b5c33650bff7d22a61c4d	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	SP1P012C_AmendmentE_vF_03-Sep-2019.pdf	277407 5f5329d2c89f3fb4f387bc4d7da43d3612526e39	no	57
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	33745 f4a95a82bf6d5d72dc6f36dadb98f5beeb6ad810	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1675190		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 05-30-2017	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: Sept 3, 2019

AMENDMENT E
WITH
REQUEST FOR CONTINUED EXAMINATION (RCE)

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Office Action mailed 7/23/19 and the Advisory Action mailed 8/13/19, please enter the following.

C

ForcePoint LLC
EX-1002
Page527

Amendments to the Claims:

The listing of amended claims follows:

1.-20. (Cancelled)

21. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors;

based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an

C

ForcePoint LLC
EX-1002
Page528

intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

22. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the intrusion prevention-type option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with intrusion prevention-type functionality such that the connection request is prevented at the particular single device.

23. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that at least two options are provided including a firewall-type option, and an intrusion prevention-type option for preventing a connection request; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the intrusion prevention-type option is applied to the plurality of devices for preventing the connection request across the plurality of devices after the receipt of the at least one occurrence packet; and the instructions are configured such that, in

C

ForcePoint LLC
EX-1002
Page529

response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device.

24. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith.

25. (Cancelled)

26. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one

C

ForcePoint LLC
EX-1002
Page530

configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;

based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

27. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page531

28. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

29. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page532

30. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

31. (Currently Amended) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

C

ForcePoint LLC
EX-1002
Page533

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

display information that is based on the first vulnerability information;

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors;

wherein the at least one configuration involves at least one operating system.

32. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence.

33. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion mitigation system-based occurrence

C

ForcePoint LLC
EX-1002
Page534

mitigation type being caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being caused at the third device in response to the occurrence.

34. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

35. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion mitigation system-based occurrence mitigation type being completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being completed at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page535

36. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion mitigation system-based occurrence mitigation type.

37. (Previously Presented) The non-transitory computer-readable media of Claim 31, wherein the intrusion mitigation system-based occurrence mitigation type includes at least one of an intrusion prevention system-based occurrence mitigation type or an intrusion detection system-based occurrence mitigation type, and the information includes a recommendation.

C

ForcePoint LLC
EX-1002
Page536

38. (Previously Presented) The non-transitory computer-readable media of Claim 26, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence.

39. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only relevant occurrence mitigation actions are available for selection by the user.

40. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the at least one accurately identified vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one accurately identified vulnerability.

41. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that different user input is allowed to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page537

42. (Previously Presented) The non-transitory computer-readable media of Claim 41, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type at the first device.

43. (Previously Presented) The non-transitory computer-readable media of Claim 41, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being rolled back at the third device.

44. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one accurately identified vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability.

45. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

C

ForcePoint LLC
EX-1002
Page538

determine the occurrence to have a first severity if it is determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence;

determine the occurrence to have a second severity if it determined that the at least one accurately identified vulnerability of the at least one of the plurality of devices is not susceptible to being taken advantage of by the occurrence; and

report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity.

46. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action.

47. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the

ForcePoint LLC
EX-1002
Page539

intrusion prevention system-based occurrence mitigation type in response to a selection of a second one of the multiple options.

48. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

49. (Previously Presented) The non-transitory computer-readable media of Claim 48, wherein the instructions are configured such that the automatic application of the first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the

C

ForcePoint LLC
EX-1002
Page540

intrusion prevention system-based occurrence mitigation type includes sending a second signal to at least one component with intrusion prevention system functionality.

50. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences.

51. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one accurately identified vulnerability while there is no installation of a patch that removes the at least one accurately identified vulnerability.

52. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device; the determining that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine whether a first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least

ForcePoint LLC
EX-1002
Page541

one first occurrence packet, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one second occurrence packet; and the allowing the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall-based occurrence mitigation type is completed by sending a first signal over at least one network to a first component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type is completed by sending a second signal to a second component with an intrusion prevention system type functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device.

53. (Previously Presented) The non-transitory computer-readable media of Claim 52, wherein the instructions are configured such that at least one of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of:

C

ForcePoint LLC
EX-1002
Page542

receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said first vulnerability information is generated via a vulnerability scan operation;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

C

ForcePoint LLC
EX-1002
Page543

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said at least one accurately identified vulnerability includes the at least one operating system;

said actual vulnerabilities include the at least one accurately identified vulnerability;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which includes the at least one

ForcePoint LLC
EX-1002
Page544

operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one aspect of the at least one first occurrence packet involves at least one of a payload thereof or an IP address;

said at least one aspect of the at least one first occurrence packet is utilized to determine whether the first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, by utilizing the at least one aspect in connection with at least one of a cross-referencing operation or a look-up operation;

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action;

said first signal and thee second signal include at least one of response signals, or signals sent in response to a query signal;

C

ForcePoint LLC
EX-1002
Page545

said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality;

said second component with the intrusion prevention system type functionality includes at least one of an intrusion prevention system, an intrusion detection system with the intrusion prevention system type functionality, a gateway with the intrusion prevention system type functionality, a router with the intrusion prevention system type functionality, a sensor with the intrusion prevention system type functionality, or a multiple-security product system with the intrusion prevention system type functionality;

said preventing includes at least one of rejecting a request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or

said automatic response includes a real-time response.

54. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information identifies at least one actual vulnerability;

C

ForcePoint LLC
EX-1002
Page546

said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is utilized for identifying the at least one operating system or an application;

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the

C

ForcePoint LLC
EX-1002
Page547

occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said at least one actual vulnerability is the at least one operating system;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first

C

ForcePoint LLC
EX-1002
Page548

aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is actually vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

C

ForcePoint LLC
EX-1002
Page549

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

55. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused.

56. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence.

C

ForcePoint LLC
EX-1002
Page550

57. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the intrusion prevention system-based occurrence mitigation type being selectively caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence.

58. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

59. (Previously Presented) The non-transitory computer-readable media of Claim 21, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

C

ForcePoint LLC
EX-1002
Page551

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said second vulnerability information includes actual vulnerability information;

said second vulnerability information includes potential vulnerability information;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information identifies at least one accurately identified vulnerability;

said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the accurately identified vulnerabilities;

said first vulnerability information includes potential vulnerability information;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is utilized for identifying the at least one operating system or an application;

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

ForcePoint LLC
EX-1002
Page552

said occurrence mitigation includes at least one of removing the at least one accurately identified vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one accurately identified vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said intrusion prevention system-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one accurately identified vulnerability after the occurrence;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different

C

ForcePoint LLC
EX-1002
Page553

occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one accurately identified vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first accurately identified vulnerability and utilizing a second one of the different occurrence mitigation actions for a second accurately identified vulnerability;

said at least one accurately identified vulnerability is the at least one operating system;

said preventing advantage being taken of the accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one accurately identified vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

ForcePoint LLC
EX-1002
Page554

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one accurately identified vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is accurately identified as being vulnerable to the at least one accurately identified vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

one of said different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

C

ForcePoint LLC
EX-1002
Page555

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

60. (New) A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including:

at least one first potential vulnerability, and

at least one second potential vulnerability;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;

based on a packet analysis, determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

ForcePoint LLC
EX-1002
Page556

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

61. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured for providing at least two options via a user interface including a firewall-type option for preventing at least one occurrence packet, and another option; the instructions are configured such that, in response to user input received prior to receipt of the at least one occurrence packet, the firewall-type option is applied to the plurality of devices by sending a first signal over at least one network to at least one first component with firewall-type functionality such that the at least one occurrence packet is prevented across the plurality of devices; and the instructions are configured such that, in response to additional user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the other option is applied to the particular single device by sending a second signal over the at least one network to at least one second component with other functionality.

62. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that at least two options are provided including a firewall-type option associated with the firewall-based occurrence mitigation type, and an other option associated with the other occurrence mitigation type; the instructions are configured such that, in response to user input prior to receipt of at least one occurrence packet, the other option is applied to the plurality of devices; and the instructions are configured such that, in response to user input after the receipt of the at least one occurrence packet in connection with a particular single device of the plurality of devices, the firewall-type option is applied to the particular single device.

C

ForcePoint LLC
EX-1002
Page557

63. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the at least one actual vulnerability is determined as a function of the at least one operating system, so that, in order to avoid false positives, only relevant vulnerabilities prompt user selection among the different occurrence mitigation actions of the diverse occurrence mitigation types in connection therewith.

64. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that which of the different occurrence mitigation actions for which one or more options are provided to a user, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that only relevant occurrence mitigation actions are available for selection by the user.

65. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the at least one actual vulnerability is determined as a function of the at least one operating system and at least one some of the different occurrence mitigation actions are specific to the at least one actual vulnerability.

66. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that different user input is permitted to be received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions, in a manner that the different user input results in: only a first occurrence mitigation action of the firewall-based occurrence mitigation type being user-selectively completed at the first device in response to the occurrence, only a second occurrence mitigation action of the other occurrence mitigation type being user-selectively completed at the second device in response to the occurrence, and both the first occurrence mitigation action and the second occurrence mitigation action being user-selectively completed at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page558

67. (New) The non-transitory computer-readable media of Claim 66, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being supplemented by the second occurrence mitigation action of the other occurrence mitigation type at the first device.

68. (New) The non-transitory computer-readable media of Claim 66, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the other occurrence mitigation type being rolled back at the third device.

69. (New) The non-transitory computer-readable media of Claim 66, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for causing completion of the different occurrence mitigation actions, in a manner that the additional user input results in: the second occurrence mitigation action of the other occurrence mitigation type being supplemented by the first occurrence mitigation action of the firewall-based occurrence mitigation type.

70. (New) The non-transitory computer-readable media of Claim 66, wherein the instructions are configured such that additional user input is permitted to be received after a reporting of the occurrence, for prompting a rollback of one or more of the different occurrence mitigation actions, in a manner that the additional user input results in: the first occurrence mitigation action of the firewall-based occurrence mitigation type being rolled back at the third device.

ForcePoint LLC
EX-1002
Page559

71. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types include: a first occurrence mitigation action of the firewall-based occurrence mitigation type including at least one of setting a configuration option, setting of a policy, or an installation of a patch; and a second occurrence mitigation action of the other occurrence mitigation type including at least one of setting the configuration option, the setting of the policy, or the installation of the patch that is different than that included in connection with the first occurrence mitigation action.

72. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that multiple options for selecting the different occurrence mitigation actions are displayed via an intrusion prevention system interface of an intrusion prevention system that is supported by a single client agent that supports at least one aspect of the identifying the occurrence, at least one aspect of automatically completing a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type in response to a selection of a first one of the multiple options, and at least one aspect of automatically completing a second one of the different occurrence mitigation actions of the other occurrence mitigation type in response to a selection of a second one of the multiple options.

73. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

display at least two options for selecting the different occurrence mitigation actions, utilizing at least one user interface;

receive a first user input selecting a first one of the options, utilizing the at least one user interface;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

C

ForcePoint LLC
EX-1002
Page560

receive a second user input selecting a second one of the options, utilizing the at least one user interface; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the other occurrence mitigation type.

74. (New) The non-transitory computer-readable media of Claim 73, wherein the instructions are configured such that the automatic application of the first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type includes sending a first signal to at least one component with firewall functionality; and the automatic application of the second one of the different occurrence mitigation actions of the other occurrence mitigation type includes sending a second signal to at least one component with other functionality.

75. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the different occurrence mitigation actions of the diverse occurrence mitigation types are for being automatically applied to different occurrences with different severities in real-time in response to the identification of the different occurrences based on a user selection of one or more options for selecting among the different occurrence mitigation actions before the identification of the different occurrences.

76. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

based on user input, automatically block the occurrence, to prevent an attack from taking advantage of the at least one actual vulnerability while there is no installation of a patch that removes the at least one actual vulnerability.

77. (New) The non-transitory computer-readable media of Claim 60, wherein the identifying the occurrence is accomplished by: identifying at least one first occurrence packet of a first

C

ForcePoint LLC
EX-1002
Page561

occurrence directed to the first device, and identifying at least one second occurrence packet of a second occurrence directed to the second device; the determining that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible is accomplished by: identifying at least one aspect of the at least one first occurrence packet and utilizing the at least one aspect of the at least one first occurrence packet to determine whether a first actual vulnerability of the first device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one first occurrence packet, and identifying at least one aspect of the at least one second occurrence packet and utilizing the at least one aspect of the at least one second occurrence packet to determine whether a second actual vulnerability of the second device identified by the first vulnerability information is configured so as to be taken advantage of by the at least one second occurrence packet; and the permitting the selective utilization of the different occurrence mitigation actions includes sending one or more control signals in response to receiving user input via a graphical user interface; wherein the instructions are configured such that, based on the user input, a first occurrence mitigation action of the different occurrence mitigation actions of the firewall-based occurrence mitigation type is completed by sending a first signal over at least one network to a first component with a firewall type functionality and preventing the first occurrence including the at least one first occurrence packet from taking advantage of the first actual vulnerability in connection with the first device; and wherein the instructions are configured such that a second occurrence mitigation action of the different occurrence mitigation actions of the other occurrence mitigation type is completed by sending a second signal to a second component with other functionality and preventing the second occurrence including the at least one second occurrence packet, in automatic response thereto, from taking advantage of the second actual vulnerability in connection with the second device.

78. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is permitted, is based on one or more of the actual vulnerabilities to

C

ForcePoint LLC
EX-1002
Page562

which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is permitted.

79. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence.

80. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively permitted for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively permitted at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the other occurrence mitigation type being selectively permitted at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively permitted at the third device in response to the occurrence.

81. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions are configured such that one or more options are provided to a user so that the user is permitted to select each of the different occurrence mitigation actions of the diverse occurrence mitigation types in connection with the at least one actual vulnerability which includes a single actual vulnerability, such that both of the different occurrence mitigation actions are associated with the single actual vulnerability.

82. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

C

ForcePoint LLC
EX-1002
Page563

determine the occurrence to have a first severity if it is determined that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence;

determine the occurrence to have a second severity if it determined that the at least one actual vulnerability of the at least one of the plurality of devices is not susceptible to being taken advantage of by the occurrence; and

report the occurrence differently based on whether the occurrence is determined to have the first severity or the second severity.

83. (New) The non-transitory computer-readable media of Claim 60, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the other occurrence mitigation type.

84. (New) The non-transitory computer-readable media of Claim 60, wherein the other occurrence mitigation type includes a scan-based occurrence mitigation type.

85. (New) The non-transitory computer-readable media of Claim 60, wherein the other occurrence mitigation type includes a patch-based occurrence mitigation type.

86. (New) The non-transitory computer-readable media of Claim 77, wherein the instructions are configured such that at least one of:

said at least one first data storage includes at least one first database;

C

ForcePoint LLC
EX-1002
Page564

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said second vulnerability information includes accurately identified vulnerability information;

said second vulnerability information includes actual vulnerability information;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information includes potential vulnerability information;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation by preventing advantage being taken includes at least one of removing the at least one actual vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one actual vulnerability;

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

C

ForcePoint LLC
EX-1002
Page565

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one actual vulnerability after the occurrence;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one actual vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said packet analysis includes an analysis involving the occurrence that involves one or more packets;

said packet analysis includes an analysis involving a behavior of one or more packets;

said packet analysis includes an analysis involving a content of one or more packets;

C

ForcePoint LLC
EX-1002
Page566

said packet analysis includes an analysis involving a header of one or more packets;

said packet analysis includes an analysis involving a payload of one or more packets;

said one or more monitors includes a single monitor;

said one or more monitors includes multiple monitors;

said one or more monitors includes at least one sensor monitor;

said one or more monitors includes at least one in-line sensor monitor;

said one or more monitors includes is in-line;

said one or more monitors includes at least one intrusion prevention system monitor;

said one or more monitors includes at least one intrusion detection system monitor;

said one or more monitors includes at least one intrusion prevention monitor;

said one or more monitors includes at least one intrusion detection monitor;

said at least one actual vulnerability includes the at least one operating system;

said actual vulnerabilities include the at least one actual vulnerability;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one actual vulnerability which includes the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

C

ForcePoint LLC
EX-1002
Page567

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said user input includes separate user input for selecting the first occurrence mitigation action and the second occurrence mitigation action;

said first signal and thee second signal include at least one of response signals, or signals sent in response to a query signal;

said first component with the firewall type functionality includes at least one of a firewall, a gateway with the firewall type functionality, a router with the firewall type functionality, a sensor with the firewall type functionality, or a multiple-security product system with the firewall type functionality;

said preventing includes at least one of rejecting a request, disallowing an attempt, dropping at least one packet, blocking a potential attack, redirecting a request, setting a policy, affecting a service, changing a configuration option, or installing a patch; or

said automatic response includes a real-time response.

87. (New) The non-transitory computer-readable media of Claim 62, wherein the instructions are configured such that each of:

said at least one first data storage includes at least one first database;

C

ForcePoint LLC
EX-1002
Page568

said at least one second data storage includes at least one second database;

said second vulnerability information is received from the at least one second data storage by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said first vulnerability information is generated via a vulnerability scan operation;

said first vulnerability information identifies at least one actual vulnerability;

said first vulnerability information includes at least one of a vulnerability identifier or information associated with one or more of the actual vulnerabilities;

said first device, said second device, and said third device are part of the same group;

said at least one configuration includes at least one of configuration data, configuration information, or a configuration status;

said at least one configuration includes at least one of a configuration option, a policy setting, or a patch;

said at least one configuration for being utilized for identifying the at least one operating system or an application;

said at least one configuration is identified utilizing information regarding the at least one operating system or an application;

said at least one configuration is identified via user input in connection with at least one setting;

said occurrence mitigation includes at least one of removing the at least one actual vulnerability, or reducing an effect of any occurrence that takes advantage of the at least one actual vulnerability;

ForcePoint LLC
EX-1002
Page569

said firewall-based occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing firewall functionality, or a type that mitigates the occurrence utilizing a firewall;

said other occurrence mitigation type includes at least one of: a type that mitigates the occurrence utilizing intrusion prevention system functionality, or a type that mitigates the occurrence utilizing an intrusion prevention system;

said different occurrence mitigation actions of the diverse occurrence mitigation types are selectively utilized across the plurality of devices to mitigate the occurrence by preventing the occurrence from taking advantage of the at least one actual vulnerability after the occurrence;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions on one of the plurality of devices and utilizing a second one of the different occurrence mitigation actions on another one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions and a second one of the different occurrence mitigation actions on each of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes completing a selected at least one of a first one of the different occurrence mitigation actions or a second one of the different occurrence mitigation actions to address the at least one actual vulnerability in connection with at least one of the plurality of devices;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first

C

ForcePoint LLC
EX-1002
Page570

actual vulnerability and utilizing a second one of the different occurrence mitigation actions for a second actual vulnerability;

said at least one actual vulnerability is the at least one operating system;

said preventing advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, includes utilizing a first one of the different occurrence mitigation actions for a first aspect of the at least one actual vulnerability which is the at least one operating system and utilizing a second one of the different occurrence mitigation actions for a second aspect of the at least one operating system;

one or more of said different occurrence mitigation actions is caused after the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

one or more of said different occurrence mitigation actions is caused before the occurrence to selectively utilize the different occurrence mitigation actions of the diverse occurrence mitigation types;

said different occurrence mitigation actions include different remediation actions;

said different occurrence mitigation actions of the diverse occurrence mitigation types utilized at the plurality of devices include the same set of said different occurrence mitigation actions;

said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack;

said at least one actual vulnerability includes at least one of the potential vulnerabilities to which the plurality of devices is determined to be actually vulnerable based on the identified at least one configuration;

C

ForcePoint LLC
EX-1002
Page571

said at least one configuration includes at least one of: service pack information, one or more elements contained in files including at least one of an *.ini or *.conf file, registry information, identification of the at least one operating system, identification of a software version, or identification of software;

said determining that the plurality of devices is actually vulnerable to the at least one actual vulnerability includes at least one of: matching the identified at least one configuration with a guideline associated with at least one update, or cross-referencing an identifier with the identified at least one configuration;

said non-transitory computer-readable media includes a single non-transitory computer readable medium;

one or more of said different occurrence mitigation actions, after a user selection, is automatically applied at a later time;

one or more of said different occurrence mitigation actions puts a policy in place for being utilized at a later time;

one or more of said different occurrence mitigation actions, after an automatic application thereof, is utilized at a later time for the occurrence mitigation;

one of said different occurrence mitigation actions of the other occurrence mitigation type utilizes an intrusion prevention system to deploy a patch;

said one or more monitors includes at least one sensor monitor;

said one or more monitors includes at least one in-line sensor monitor;

said one or more monitors includes is in-line;

said one or more monitors includes at least one intrusion prevention system monitor;

said one or more monitors includes at least one intrusion detection system monitor;

C

ForcePoint LLC
EX-1002
Page572

said one or more monitors includes at least one intrusion prevention monitor;

said one or more monitors includes at least one intrusion detection monitor;

one of said different occurrence mitigation actions of the firewall-based occurrence mitigation type utilizes a firewall to deploy a patch utilizing an update component; and

wherein the instructions are configured for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation, and wherein the instructions are configured for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

88. (New) The non-transitory computer-readable media of Claim 62, wherein the instructions are configured such that which of the different occurrence mitigation actions for which selective utilization is caused, is based on one or more of the actual vulnerabilities to which the plurality of devices is actually vulnerable so that utilization of only relevant occurrence mitigation actions is caused.

89. (New) The non-transitory computer-readable media of Claim 62, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence.

90. (New) The non-transitory computer-readable media of Claim 62, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is selectively caused for different devices prior to the occurrence, resulting in: the utilization of only a first occurrence mitigation action of the firewall-based occurrence mitigation type being selectively caused at the first device in response to the occurrence, the utilization of only a second occurrence mitigation action of the other occurrence mitigation type being selectively caused at the second device in response to the occurrence, and the utilization of both the first occurrence mitigation action and the second occurrence mitigation action being selectively caused at the third device in response to the occurrence.

C

ForcePoint LLC
EX-1002
Page573

91. (New) The non-transitory computer-readable media of Claim 62, wherein the instructions, when executed by the one or more processors, cause the one or more processors to:

receive a first user input;

based on the first user input, automatically apply a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type;

receive a second user input; and

based on the second user input, automatically apply a second one of the different occurrence mitigation actions of the other occurrence mitigation type.

C

ForcePoint LLC
EX-1002
Page574

Remarks:

The claims have been clarified. Specifically, Claims 60-91 have been added.

Claims 21-46 and 48-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more. Specifically, in the latest Office Action mailed 7/23/2019, the Examiner argues that "[o]ther than the recitation of one or more processors to perform the limitations, nothing in the claims limitations precludes the limitations from being performed in mind." Applicant respectfully disagrees.

Argument #1

First, with respect to Claim 21, for example, the following emphasized claim terms can NOT be performed in mind:

> "**identify an occurrence in connection with at least one of the plurality of devices;**
> **determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information**; and
> permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for **occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices**" (emphasis added).

Clearly, a person's "mind" cannot: determine that at least one accurately identified vulnerability is susceptible to being taken advantage of by an occurrence identified, utilizing the first vulnerability information; and prevent advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across devices, in the specific context claimed.

C

ForcePoint LLC
EX-1002
Page575

In a similar context in *SRI International, Inc. v. Cisco Systems, Inc*. (Fed. Cir. 2019), the Federal Circuit confirmed the District Court's Step One determination that "claim 1 is not directed to an abstract idea" because the "claims are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: **identifying hackers or potential intruders into the network**" (emphasis added).

In explanation, the Federal Circuit opinion states:

> "…the claims here are not directed to using a computer as a tool—that is, automating a conventional idea on a computer. Rather, the representative claim improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security.
>
> Indeed, **we tend to agree with [Plaintiff] that the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets** ..." (emphasis added).

Thus, similar to *SRI International*, the current claims recite security-related activity that simply cannot be performed by the human mind, and, thus, the current claims are not directed to an abstract idea.

In the Advisory mailed 8/13/2019, the Examiner argues that "unlike the cited [*SRI International*] case, the highlighted limitations of the claims in the instant application do not recite network monitors or analyzing network packets." Applicant respectfully disagrees with this attempt to distinguish *SRI International*. Nevertheless, applicant has amended at least some of the claims to further align the claims of the instant application with those in *SRI International*, in the manner highlighted by the Examiner.

Argument #2

Second, it appears the Examiner *did not even address* applicant's arguments with respect to Step 2 of the *Alice* test.

C

ForcePoint LLC
EX-1002
Page576

Specifically, in the present application, even if the Examiner were to conclude that the claims fall within the appropriate groupings of abstract ideas, the claims in the present application include one or more additional elements that extend beyond the judicial exception(s) and integrate the exception into a practical application. See the highlighted language below, just by way of example in the context of Claim 21, that represents an *improvement in the functioning of a computer* or *technical field* so as to *render the same* a *particular machine* (or method for operating the same) in a *particular technological environment.*

> "21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:
>
> receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including:
>
> at least one first potential vulnerability, and
>
> at least one second potential vulnerability;
>
> said first vulnerability information generated utilizing the second vulnerability information, by:
>
> **identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and**
>
> **determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities**;
>
> identify an occurrence in connection with at least one of the plurality of devices;
>
> **determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information**; and
>
> **permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices**;
>
> wherein the at least one configuration involves **at least one operating system**." (emphasis added)

ForcePoint LLC
EX-1002
Page577

In the Advisory mailed 8/13/2019, the Examiner simply regurgitates previous arguments that "[t]he claims do not recite any additional elements other than a processor at a high level of generality. The use of the processor at a high level of generality amounts to no more than mere instructions being applied to the exception using a generic computer component." However, in doing so, the Examiner has simply ignored the highlighted claim terms above.

Further, applicant respectfully notes that, in the recent USPTO Guidance, the USPTO indicated, for Step 2 of the *Alice* test, that if the Examiner concludes, under the Guidance, that an additional element is insignificant extra-solution activity, they should reevaluate that conclusion in Step 2 of the *Alice* test. If such reevaluation indicates that the element is *unconventional or otherwise more than what is well-understood, routine, conventional activity in the field*, this finding may indicate that an inventive concept is present and that the claim is thus eligible.

In the present case, even if the Examiner concludes that the above-highlighted elements are insignificant extra-solution activity, they are indeed unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, for at least the reason that the claim elements, individually and in combination, are not found in the prior art. Further, as evidenced below, the Examiner's cited art is <u>not</u> even prior art, despite the allegations to the contrary in the Advisory mailed 8/13/2019.

Claims 21, 24, 26, 32, 37, 39, 40, 41, 43 and 45 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over US 7181769 to Keanini et al (hereinafter Keanini) and US 7509681 to Flowers et al (hereinafter Flowers). Specifically, in the latest Office Action mailed 7/23/2019, the Examiner argues that "US provisional application 60/338078 provides … support to the cited subject matter." Applicant respectfully disagrees.

<u>Argument #1</u>

In particular, with respect to Claim 21, the Examiner appears to rely on "Block on Exposure: Page 5, 4.2, 4th para; 4.2.1- block action taken; Page 7; page 8: 6.1: Action; IP360 Concepts

C

ForcePoint LLC
EX-1002
Page578

Guide Paper: page 8, section 1.4.2.3; pages 10-11, section 2.2." to make a prior art showing of applicant's claimed technique to "permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices."

In doing so, the Examiner admits that "Keanini teaches a firewall-based occurrence mitigation type but does not explicitly teach a other occurrence mitigation type." However, simply disclosing a firewall in the forgoing Keanini excerpts does not meet applicant's claimed technique to "**permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types**, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities **utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices**," in the specific context claimed (emphasis added).

In the Advisory mailed 8/13/2019, the Examiner argues that "Keanini teaches: column 11, lines 15-25: The event daemon module 820 performs a set of actions to block a host's exposure to its vulnerabilities. In one embodiment the event daemon module 820 responds to a notification of vulnerabilities from the device profiler 165. In another embodiment, the event daemon module 820 responds to a notification of a real-time attack from the traffic monitor 185. The blocking actions may include configuring a firewall to halt communication between the enterprise network 115 and the WAN 130, closing open ports on the host 191, and/or preventing the operating systems and/or applications from executing programs (different occurrence mitigation actions of diverse occurrence mitigation types)."

C

ForcePoint LLC
EX-1002
Page579

Applicant respectfully disagrees. Specifically, applicant acknowledges that Keanini claims to be "a continuation-in-part of U.S. patent application Ser. No. 09/757,963 filed on Jan. 10, 2001 now U.S. Pat. No. 6,957,348, Ser. No. 09/757,872 filed on Jan. 10, 2001 and Ser. No. 09/648,211 filed on Aug. 25, 2000 now U.S. Pat. No. 7,073,198." However, none of the above priority documents above disclose all of the subject matter in Keanini that is relied upon by the Examiner in attempting to meet applicant's claims, namely column 11, lines 15-25 from Keanini.

Still yet, Applicant acknowledges that Keanini purportedly claims the benefit of "U.S. Provisional Application No. 60/388,078, filed on Jun. 11, 2002." However, the aforementioned provisional does not disclose all of the subject matter in Keanini that is relied upon by the Examiner in an attempt to meet applicant's claims, namely column 11, lines 15-25 from Keanini.

To this end, the teachings of Keanini relied upon by the Examiner (namely column 11, lines 15-25 from Keanini) do not enjoy a priority date that precedes the priority of the instant application that was established earlier.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. With respect to the other independent claims (other than Claim 21), applicant respectfully asserts that such claims are

C

ForcePoint LLC
EX-1002
Page580

deemed allowable for reasons similar, but not necessarily identical, to one or more of the aforementioned reasons (see each claim for specific claim language contained therein).

Argument #2

Second, it appears the Examiner *did not even address* applicant's arguments that Keanini does not include a claim that is actually entitled to the benefit of priority of the provisional application. See the combination of terms highlighted from the independent claims from Keanini below:

> 1. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host, wherein a determined vulnerability pertains to a specific location and wherein the traffic monitor monitors for exploits of the determined vulnerability directed to the location and ignores exploits of the determined vulnerability directed to locations to which the determined vulnerability does not pertain. (emphasis added)
>
> 9. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**; a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host; and a centralized correlation server, communicatively coupled with the network at a centrally accessible location, the device profiler and the traffic monitor, the centralized correlation server for receiving the determined vulnerabilities from the device profiler, identifying signatures of network traffic indicating attacks exploiting the determined vulnerabilities, and sending the signatures to the traffic monitor. (emphasis added)
>
> 16. A distributed computer network security system for detecting an attack on a host on a network having a plurality of hosts, the system comprising: a device profiler

C

ForcePoint LLC
EX-1002
Page581

> communicatively coupled with the network, the device profiler for identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**, the device profiler including a low-level sensor for sending anomalous data packets to the host and determining the characteristics based on the host's response to the anomalous data packets; and a traffic monitor, communicatively coupled with the network and the device profiler, and cooperative with the device profiler, for monitoring the network for traffic indicative of an attack on the host, from the plurality of hosts on the network, exploiting one of the determined vulnerabilities of the host. (emphasis added)

In the Advisory mailed 8/13/2019, the Examiner argues that "it is unclear why Keanini's claims are under scrutiny when support for the subject matter cited in rejecting the claims has been shown to be present in the provisional application 60/388078." In response, applicant reiterates that Keanini is not proper prior art under *Dynamic Drinkware, LLC v. National Graphics, Inc*., 800 F.3d 1375 (Fed. Cir. 2015), as a reference patent is only entitled to claim the benefit of the filing date of its provisional application if the disclosure of the provisional application provides support for the claims in the reference patent in compliance with § 112, ¶ 1. See MPEP 706.

In view of the above, Keanini can only rely on its June 6, 2003 filing date, which post-dates September 27, 2002, a date (but not necessarily the earliest date) as of which the claimed invention in the present application was conceived of and actually reduced to practice. Thus, Keanini is not prior art.

In the Advisory mailed 8/13/2019, the Examiner attempts to show support in U.S. Provisional Application No. 60/388,078 for the claimed "identifying characteristics of a host from the plurality of hosts on the network and determining vulnerabilities of the host based on the characteristics **according to a tree-structured vulnerability table**," in the specific context claimed (emphasis added). It should be noted that the Examiner's cited "list of vulnerabilities" simply does not rise to the level of specificity of the claimed "**tree-structured vulnerability table**," in the specific context claimed (emphasis added). Further, there is no teaching of the specific context in which the "**tree-structured vulnerability table**" is claimed, namely,

ForcePoint LLC
EX-1002
Page582

"**determining vulnerabilities of the host based on the characteristics according to a tree-structured vulnerability table**," in the specific context claimed (emphasis added).

It is believed that all of the pending issues have been addressed. The claims are in condition for allowance. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, it should be noted that no claim is intended to be construed under 35 U.S.C. 112, paragraph 6.

Should the Examiner deem that any further amendment is desirable to place this Application in condition for allowance, Applicant invites the Examiner to telephone the undersigned attorney at the number listed below.

Respectfully submitted,



Dated: 03 Sep 2019

Patrick E. Caldwell, Esq.
Reg. No. 44,580

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

C

ForcePoint LLC
EX-1002
Page583

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/608,978	Filing Date 05/30/2017	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	09/03/2019	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 69	Minus	** 69	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/HALLEY D MASSEY/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P012C	Application No. 15/608,978
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Inventor Brett M. Oliphant	Confirmation Number 9647
		Filing Date 05/30/2017	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	A	Notice of Appeal Filed 11/25/2019 for USPAN 15/608,981
	B	Advisory Action Filed 8/13/2019 for USPAN 15/608,981
	C	Notice of Allowance Mailed 9/24/2019 for USPAN 15/608,983

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-12-19
Name/Print	Patrick Caldwell	Registration Number	44580

Electronic Acknowledgement Receipt	
EFS ID:	38093677
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	19-DEC-2019
Filing Date:	30-MAY-2017
Time Stamp:	17:38:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	SP1P012C_IDS_XMTL_20191219_vF.pdf	54980 8e22bcc34615d8da226e7231f8c2abcaa87a2a8c	no	2

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	SP1P012C_IDS_1449_20191219_vF.pdf	56350 7cc69a5fe099966fed2651703049bac0c000c5c0	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Non Patent Literature	15608981.pdf	198283 7d9eb6660c062b7ea8ce266b26aa9e97aa0b14d5	no	2
Warnings:					
Information:					
4	Non Patent Literature	15608981_1.pdf	289084 29b948ff984db285991a54616a1efd68cfc2aa11	no	4
Warnings:					
Information:					
5	Non Patent Literature	15608983.pdf	479176 90688051ba63caf002d4b582926c4abcb0f91ec4	no	11
Warnings:					
Information:					
		Total Files Size (in bytes):	1077873		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 2017-05-30	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: Dec 19, 2019

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(b)

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

ForcePoint LLC
EX-1002
Page589

Additionally, related patent U.S. Patent No. 8984644 is the subject of an appeal (US Court of Appeals for the Federal Circuit Case 2019-1881).

This Information Disclosure Statement is being filed after the mailing date of a RCE. Accordingly, no fee is due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-4964 (Order No. SP1P012C).

Respectfully submitted,



Dated: 19 Dec 2019

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

ForcePoint LLC
EX-1002
Page590

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

92045 7590 01/15/2020

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER	
HERZOG, MADHURI R	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/15/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

TITLE OF INVENTION: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	04/15/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

C

ForcePoint LLC
EX-1002
Page591

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

92045 7590 01/15/2020
The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

TITLE OF INVENTION: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	04/15/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
HERZOG, MADHURI R	2438	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

ForcePoint LLC
EX-1002
Page592

C

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

92045 7590 01/15/2020

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

EXAMINER	
HERZOG, MADHURI R	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/15/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

C

ForcePoint LLC
EX-1002
Page593

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ForcePoint LLC
EX-1002
Page594

Notice of Allowability	Application No. 15/608,978	Applicant(s) Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 09/03/2019.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 21-24 and 26-91 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 12/19/2019.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

C

ForcePoint LLC
EX-1002
Page595

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 21-24 and claims 26-91, now renumbered as claims 1-70, have been examined.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/19/2019 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Allowable Subject Matter

6. Claims 21-24 and claims 26-91 are allowed over prior art of record.

Response to Arguments

7. Applicant's arguments, see Remarks, filed 09/03/2019, have been fully considered and are persuasive.

ForcePoint LLC
EX-1002
Page596

Examiner's Statement of Reasons for Allowance

8. The following is an examiner's statement of reasons for allowance:

Independent claims 21, 26, 31 and 60 are allowed in view of reasons presented by the applicant in the Remarks. Claims 22-24, 26, 27-30, 32-59 and 61-91 depend on one of the above independent claims and are therefore, allowed by virtue of their dependency.

Prior art of record Flowers teaches: A vulnerability detection system (VDS) (1) gathers information about network 100 and (2) processes that information to determine vulnerabilities. The VDS contains a rules database that contains rules that describe vulnerabilities and provide a programmatic means to check for the presence of those vulnerabilities. In particular, the information received from a network as a result of reflex testing is checked against the rules database and can be used to detect every device in the network, identify each host's operating system as well as the open ports of the host and the applications being run on them. This information is then used to identify vulnerabilities. An intrusion detection system (IDS) examines network traffic for signs of malicious activity. The rules used by the IDS are determined by the VDS vulnerability analysis, so that only rules that describe possible intrusion conditions as they exist for the specific network are loaded. Such a Target-based IDS monitors for specific conditions to which the network has been determined to be vulnerable, as well as any range of conditions or attacks to which the network might be vulnerable.

However, Flowers fail to teach: "identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors; based on a

ForcePoint LLC
EX-1002
Page597

packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type", i.e., Flowers teaches monitoring for attacks based on vulnerabilities identified in the network but does not teach identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 6301668 to Gleichauf et al: A method and system for adaptive network security using network vulnerability assessment is disclosed. The method comprises

ForcePoint LLC
EX-1002
Page598

directing a request onto a network. A response to the request is assessed to discover network information. A plurality of analysis tasks are prioritized based upon the network information. The plurality of analysis tasks are to be performed on monitored network data traffic in order to identify attacks upon the network.

Managing Cyber Security Vulnerabilities in Large Networks by Chang et al: In this paper, we describe a methodology for statistical sampling and analysis, combined with a network and host security discipline for developing Lucent's cyber security profile in an effective, efficient manner. We have also developed a methodology for correlating vulnerabilities in and among the network and operating systems. We found the distribution of high-risk vulnerabilities to be very concentrated. Through root cause analyses, we developed a focused plan for mitigating vulnerabilities effectively and efficiently.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI R HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on 8:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

ForcePoint LLC
EX-1002
Page599

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MADHURI R. HERZOG
Primary Examiner
Art Unit 2438

/MADHURI R HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1002
Page600

Notice of References Cited	Application/Control No. 15/608,978	Applicant(s)/Patent Under Reexamination Oliphant et al.	
	Examiner MADHURI R HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6301668-B1	10-2001	Gleichauf; Robert E.	H04L41/12	726/22
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Chang, Edward S., et al. "Managing cyber security vulnerabilities in large networks." Bell Labs technical journal 4.4 (1999): 252-272 . (Year: 1999)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

CPC - Searched*		
Symbol	Date	Examiner
H04L 63/02$, 63/14$, 63/20$	12/18/2019	M.H
G06F 21/5$	12/18/2019	M.H

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search, Assignee search	12/18/2019	M.H
East search	12/18/2019	M.H
Google Scholar Search	12/18/2019	M.H
Consulted QAS Tod Swann	12/18/2019	M.H
Consulted TC 2400 101 QAS	12/18/2019	M.H
Search terms: determine, detect, find, discover, uncover, analyze, examine, check, vulnerability, exploit, device, node, host, terminal, client, configuration, operation, system, os, attack, intrusion, ddos, occurrence, event, malicious, suspicious, suspect, pernicious, traffic, packet, malware, threat, firewall, ids, detection, system, prevention, choose, select, designate, pick, identify, base, depend, mitigation, patch, hotfix, remediation	12/18/2019	M.H

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page602

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	Art Unit
	MADHURI R HERZOG	2438

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
H04L	63/02$, 63/14$, 63/20$ with the above search terms	12/18/2019	M.H
G06F	21/5$ with the above search terms	12/18/2019	M.H

/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	

ForcePoint LLC
EX-1002
Page603

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

CPC							
Symbol						**Type**	**Version**
H04L	/	63	/	1433		F	2013-01-01
G06F	/	21	/	57		I	2013-01-01
H04L	/	63	/	145		I	2013-01-01
H04L	/	63	/	14		I	2013-01-01
G06F	/	21	/	554		I	2013-01-01
H04L	/	63	/	1408		I	2013-01-01
H04L	/	63	/	02		I	2013-01-01
H04L	/	63	/	1441		I	2013-01-01
G06F	/	21	/	577		I	2013-01-01
G06F	/	21	/	50		I	2013-01-01
H04L	/	63	/	1416		I	2013-01-01
H04L	/	63	/	20		I	2013-01-01
H04L	/	63	/	0227		I	2013-01-01
G06F	/	21	/	55		I	2013-01-01
H04L	/	63	/	0263		A	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	70	
/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	18 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	21	6

U.S. Patent and Trademark Office — Part of Paper No.: 20191218

C

ForcePoint LLC
EX-1002
Page604

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L29/06	/	29	/	06
G06F21/57	/	21	/	57
G06F21/55	/	21	/	55
G06F21/50	/	21	/	50

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	70	
/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	18 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	21	6

U.S. Patent and Trademark Office — Part of Paper No.: 20191218

C

ForcePoint LLC
EX-1002
Page605

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		13		25	16	37	28	49	40	61	52	73	64	85
	2		14	5	26	17	38	29	50	41	62	53	74	65	86
	3		15	6	27	18	39	30	51	42	63	54	75	66	87
	4		16	7	28	19	40	31	52	43	64	55	76	67	88
	5		17	8	29	20	41	32	53	44	65	56	77	68	89
	6		18	9	30	21	42	33	54	45	66	57	78	69	90
	7		19	10	31	22	43	34	55	46	67	58	79	70	91
	8		20	11	32	23	44	35	56	47	68	59	80		
	9	1	21	12	33	24	45	36	57	48	69	60	81		
	10	2	22	13	34	25	46	37	58	49	70	61	82		
	11	3	23	14	35	26	47	38	59	50	71	62	83		
	12	4	24	15	36	27	48	39	60	51	72	63	84		

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	70	
/MADHURI R HERZOG/ Primary Examiner, Art Unit 2438	18 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	21	6

U.S. Patent and Trademark Office — Part of Paper No.: 20191218

ForcePoint LLC
EX-1002
Page606

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019	07/18/2019	12/18/2019				
	1	-	-	-	-	-				
	2	-	-	-	-	-				
	3	-	-	-	-	-				
	4	-	-	-	-	-				
	5	-	-	-	-	-				
	6	-	-	-	-	-				
	7	-	-	-	-	-				
	8	-	-	-	-	-				
	9	-	-	-	-	-				
	10	-	-	-	-	-				
	11	-	-	-	-	-				
	12	-	-	-	-	-				
	13	-	-	-	-	-				
	14	-	-	-	-	-				
	15	-	-	-	-	-				
	16	-	-	-	-	-				
	17	-	-	-	-	-				
	18	-	-	-	-	-				
	19	-	-	-	-	-				
	20	-	-	-	-	-				
1	21	✓	✓	✓	✓	=				
2	22	✓	✓	✓	✓	=				
3	23	✓	✓	✓	✓	=				
4	24	✓	✓	✓	✓	=				
	25	✓	-	-	-	-				
5	26	✓	✓	✓	✓	=				
6	27	✓	✓	✓	✓	=				
7	28	✓	✓	✓	✓	=				
8	29	✓	✓	✓	✓	=				
9	30	✓	✓	✓	✓	=				
10	31	✓	✓	✓	✓	=				
11	32	✓	✓	✓	✓	=				
12	33	✓	✓	✓	✓	=				
13	34	✓	✓	✓	✓	=				
14	35	✓	✓	✓	✓	=				
15	36	✓	✓	✓	✓	=				
16	37	✓	✓	✓	✓	=				
17	38		✓	✓	✓	=				
18	39		✓	✓	✓	=				
19	40		✓	✓	✓	=				
20	41		✓	✓	✓	=				
21	42		✓	✓	✓	=				

C

ForcePoint LLC
EX-1002
Page607

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/608,978	Oliphant et al.
	Examiner	**Art Unit**
	MADHURI R HERZOG	2438

CLAIM		DATE								
Final	Original	06/19/2018	10/30/2018	05/03/2019	07/18/2019	12/18/2019				
22	43		✓	✓	✓	=				
23	44		✓	✓	✓	=				
24	45		✓	✓	✓	=				
25	46		✓	✓	✓	=				
26	47		✓	✓	✓	=				
27	48		✓	✓	✓	=				
28	49		✓	✓	✓	=				
29	50		✓	✓	✓	=				
30	51		✓	✓	✓	=				
31	52		✓	✓	✓	=				
32	53		✓	✓	✓	=				
33	54		✓	✓	✓	=				
34	55		✓	✓	✓	=				
35	56		✓	✓	✓	=				
36	57		✓	✓	✓	=				
37	58		✓	✓	✓	=				
38	59		✓	✓	✓	=				
39	60					=				
40	61					=				
41	62					=				
42	63					=				
43	64					=				
44	65					=				
45	66					=				
46	67					=				
47	68					=				
48	69					=				
49	70					=				
50	71					=				
51	72					=				
52	73					=				
53	74					=				
54	75					=				
55	76					=				
56	77					=				
57	78					=				
58	79					=				
59	80					=				
60	81					=				
61	82					=				
62	83					=				
63	84					=				
64	85					=				
65	86					=				
66	87					=				
67	88					=				
68	89					=				
69	90					=				
70	91					=				

ForcePoint LLC
EX-1002
Page608

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office **Information Disclosure Statement by Applicant** (Use several sheets if necessary) (37 CFR §1.98(b))	Attorney Docket No. SP1P012C	Application No. 15/608,978
	Inventor Brett M. Oliphant	Confirmation Number 9647
	Filing Date 05/30/2017	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	A	Notice of Appeal Filed 11/25/2019 for USPAN 15/608,981
	B	Advisory Action Filed 8/13/2019 for USPAN 15/608,981
	C	Notice of Allowance Mailed 9/24/2019 for USPAN 15/608,983

/MADHURI R HERZOG/

01/06/2020

Substitute Disclosure Form (PTO-1449)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		SP1P012C	15/608,978
		Inventor: Brett M. Oliphant	Confirmation Number: 9647
		Filing Date: 05/30/2017	Group Art Unit: 2438

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed _____ and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2019-12-19
Name/Print	Patrick Caldwell	Registration Number	44580

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.R.H/

ForcePoint LLC
EX-1002
Page610

Sp 800-30. risk management guide for information technology **systems**

G Stoneburner, AY Goguen, A Feringa - 2002 - dl.acm.org

... The DAA or **system** authorizing official is responsible for **determining** whether the remaining risk is at an acceptable level or whether ... Step 7. Risk **Determination** Risks and Associated Risk Levels ... In **assessing** risks for an IT **system**, the first step is to define the scope of the effort ...

☆ 99 Cited by 1480 Related articles All 124 versions »

Theory and practice in **assessing vulnerability** to climate change andFacilitating adaptation

PM Kelly, WN Adger - Climatic change, 2000 - Springer

... analysis of vulnerabil- ity provides a starting point for the **determination** of effective ... or intensity, because sea surface temperature plays an important role in **determining** whether or not ... **ASSESSING VULNERABILITY** TO CLIMATE CHANGE AND FACILITATING ADAPTATION 339 ...

☆ 99 Cited by 1824 Related articles All 15 versions »

Specification-**based** anomaly detection: a new approach for **detecting** network intrusions

R Sekar, A Gupta, J Frullo, T Shanbhag... - Proceedings of the 9th ..., 2002 - dl.acm.org

... We **identify** two cate- gories of properties: • Type 1: whether a particular transition on ... 4.2 Learning statistical properties Anomaly detection is concerned with **detecting** "unusual behav- iors ... **machine** models, we are ultimately mapping behaviors to transitions of the state **machine** ...

☆ 99 Cited by 512 Related articles All 19 versions »

Modeling complex control **systems** to **identify** remotely accessible **devices** vulnerable to cyber attack

DC de Leon, J Alves-Foss, A Krings... - ACM Workshop on ..., 2002 - Citeseer

... implemented in Prolog, with resulting queries and outputs useful in **assessing** access **vulnerability** ... any mechanism capable of circuit switching, analog or digital metering, **calculating** data values ... and conducting some experiments with real data in order to **determine** the usability ...

☆ 99 Cited by 34 Related articles All 8 versions »

Toward a secure **system** engineering methodolgy

C Salter, OS Saydjari, B Schneier, J Wallner - Proceedings of the 1998 ..., 1998 - nspw.org

... a methodology for enumerating the vuinerabilities of a **system**, and **determining** what countermeasures ... First, the **system** engineer derives the list of possible adversaries **determined** by who ... tolerance **determines** what they are wiUing to do, and objectives **determine** what they ...

☆ 99 Cited by 150 Related articles All 7 versions »

Managing cyber security **vulnerabilities** in large networks

ES Chang, AK Jain, DM Slade... - Bell Labs technical ..., 1999 - Wiley Online Library

... The traditional approach to cyber security is to **identify** all **vulnerabilities**, assess their risks ... The underlying methodologies of this **finding** and others were described in detail in two ... Although different terms—such as **machine**, station, node, firewall, and router—have been used to ...

☆ 99 Cited by 20 Related articles All 2 versions »

An Introduction to the OCTAVESM Method

C Alberts, A Dorofee - white paper, CERT, http://www. cert. org ..., 2001 - sis.ashesi.edu.gh

... have been identified, an organization is positioned to analyze the information and to **identify** the information ... The goal is to **determine** how specific threats affect specific assets ... **Assessing** information security risks can be more difficult than **assessing** other types of risk because ...

☆ 99 Cited by 62 Related articles »

Concerns about intrusions into remotely accessible substation controllers and SCADA **systems**

P Oman, E Schweitzer, D Frincke - ... of the Twenty-Seventh Annual Western ..., 2000 - Citeseer

... In this paper we **identify** specific threats and discuss **mitigating** mechanisms to reduce **vulnerability** against ... a login dialog has been acquired the intruder uses social engineering to **determine** login information ... 5.3 hours, which is still not a serious obstacle for a **determined** hacker ...

☆ 99 Cited by 82 Related articles All 5 versions »

ForcePoint LLC
EX-1002
Page611

Guidelines for **assessing** the sources of risk and **vulnerability**

K Heltzmann, RS Canagarajah... - WB Social Protection ..., 2002 - www-wds.worldbank.org

... 3. **ASSESSING** THE SOURCES OF **VULNERABILITY**: THE WAY FORWARD..30 ... is the forward-looking state of expected outcomes, which are in themselves **determined** by the ... There are no general rules that **determine** a priori which risk management strategies are preferable ...

☆ 99 Cited by 123 Related articles All 12 versions »

Proton testing of SEU **mitigation** methods for the Virtex FPGA

C Carmichael, E Fuller, J Fabula ... - ... Logic Devices MAPLD, 2001 - researchgate.net

... to be halted on failure and then the bitstream could be read to **determine** how many bit ... Figure 9: This plot is obtained by **calculating** the hypothetical sensitive volume of the XQVR300 as the ... LET threshold **determined** in the heavy ion test proved the part is sensitive to the proton ...

☆ 99 Cited by 82 Related articles All 7 versions »

ForcePoint LLC
EX-1002
Page612

Bibliographic Data

Application No: 15/608,978

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /MADHURI R HERZOG/ Examiner's Signature | Initials

Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/30/2017	726	2438	SP1P012C
RULE			

APPLICANTS

SecurityProfiling, LLC, Woodville, TX,

INVENTORS

Brett M. Oliphant Plano, TX, UNITED STATES

John P. Blignaut West Lafayette, IN, UNITED STATES

CONTINUING DATA

This application is a CON of 14816931 08/03/2015 PAT 10050988

14816931 is a CON of 14499230 09/28/2014 PAT 9100431

14499230 is a CIP of 14138014 12/21/2013 PAT 9117069

14138014 is a CON of 10882852 07/01/2004ABN

10882852 has PRO of 60484085 07/01/2003

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

06/12/2017

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229
UNITED STATES

FILING FEE RECEIVED

$730

ForcePoint LLC
EX-1002
Page614

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S32	15	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (actual or real or definite) near5 (vulnerabilit$4 or exploit) with (potential or possible or probable or likely) near5 (vulnerabilit$4 or exploit) with (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 14:45
S33	159	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (actual or real or definite) near5 (vulnerabilit$4 or exploit) with (potential or possible or probable or likely) near5 (vulnerabilit$4 or exploit)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 14:52
S34	66	S33 and (vulnerabilit$4 or exploit) with (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 14:54
S35	169	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (actual or real or definite or confirmed) near5 (vulnerabilit$4 or exploit) with (potential or possible or probable or likely or raw) near5 (vulnerabilit$4 or exploit)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 15:05
S36	71	S35 and (vulnerabilit$4 or exploit) with (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 15:06
S37	68	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S36	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/17 16:39
S38	295	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (vulnerabilit$4 or exploit) with (device or node or terminal or host or client) and (determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (attack$4 or intrusion or ddos or dos or occurrence or event) with (advantage or susceptib$6 or vulnerable or expos$4 or liab$6) with (vulnerabilit$4 or exploit) and (firewall) and (ids or intrusion near3 (prevent$4 or detect$4) or ips)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:19
S39	127	S38 and (determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or	US-PGPUB; USPAT;	ADJ	ON	2019/12/18 11:21

ForcePoint LLC
EX-1002
Page615

		examin$6 or check$4) with (operating near3 system or os) with (device or node or terminal or host or client)	EPO; JPO; DERWENT; IBM_TDB			
S40	126	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S39	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:23
S41	60	S39 and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4) with (operating system or os)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:27
S42	86	S39 and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:28
S43	126	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (vulnerabilit$4 or exploit) with (device or node or terminal or host or client) with (configurat$4 or operating near2 system or os) and (determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (attack$4 or intrusion or ddos or dos or occurrence or event) with (advantage or susceptib$6 or vulnerable or expos$4 or liab$6) with (vulnerabilit$4 or exploit) and (firewall) and (ids or intrusion near3 (prevent$4 or detect$4) or ips)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:30
S44	514	(determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (vulnerabilit$4 or exploit) with (device or node or terminal or host or client) with (configurat$4 or operating near2 system or os) and (determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (attack$4 or intrusion or ddos or dos or occurrence or event or (malicious or suspicious or suspect or pernicious) near5 (traffic or packet) or malware) with (device or node or terminal or host or client) and (firewall) and (ids or intrusion near3 (prevent$4 or detect$4) or ips)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:41
S45	259	S44 and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:43
S46	230	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and S45	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2019/12/18 11:44

EAST Search History (Interference)

ForcePoint LLC
EX-1002
Page616

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S47	13	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and ((determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (vulnerabilit$4 or exploit) with (device or node or terminal or host or client) with (configurat$4 or operating near2 system or os) and (determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (attack$4 or intrusion or ddos or dos or occurrence or event or (malicious or suspicious or suspect or pernicious) near5 (traffic or packet) or malware) with (device or node or terminal or host or client) and (firewall) and (ids or intrusion near3 (prevent$4 or detect$4) or ips) and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4)).clm.	USPAT	ADJ	ON	2019/12/18 11:50
L1	3	(H04L63/02$ or H04L63/14$ or H04L63/20$ or G06F21/5$).cpc. and ((determin$5 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (vulnerabilit$4 or exploit) with (device or node or terminal or host or client) with (configurat$4 or operating near2 system or os) and (determin$6 or detect$4 or find$4 or discover$4 or uncover$4 or analy$4 or examin$6 or check$4) with (threat) with (device or node or terminal or host or client) and (firewall) and (ids or intrusion near3 (prevent$4 or detect$4) or ips) and (choos$4 or select$4 or pick$4 or designat$4 or identify$4 or identification or bas$4 or depend$4) with (mitigat$4 or patch$4 or hot$2fix$4 or remediat$4)).clm.	USPAT	ADJ	ON	2019/12/18 12:00

12/18/2019 2:02:18 PM
C:\Users\mherzog\Documents\EAST\Workspaces\App15608978.wsp

ForcePoint LLC
EX-1002
Page617

Electronic Patent Application Fee Transmittal

Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	1	50	50
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**50**

Electronic Acknowledgement Receipt	
EFS ID:	38599629
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	14-FEB-2020
Filing Date:	30-MAY-2017
Time Stamp:	23:38:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$50
RAM confirmation Number	E20202DN38539906
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	30460 3f8d222ffbb8b16d8d18f9858aa1bba78baf4ed2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	30460		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 9647
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 15/608,978	Art Unit: 2438
File Date: 2017-05-30	Docket No.: SP1P012C
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: Feb 14, 2020

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE UNDER 37 C.F.R. § 1.104(e)

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Examiner:

In response to the Notice of Allowance dated 01/15/2020, please enter the following remarks.

C

ForcePoint LLC
EX-1002
Page622

Remarks:

The Examiner has stated the following in the Examiner's Statement of Reasons for Allowance:

> Independent claims 21, 26, 31 and 60 are allowed in view of reasons presented by the applicant in the Remarks. Claims 22-24, 26, 27-30, 32-59 and 61-91 depend on one of the above independent claims and are therefore, allowed by virtue of their dependency.
>
> Prior art of record Flowers teaches: A vulnerability detection system (VDS) (1) gathers information about network 100 and (2) processes that information to determine vulnerabilities. The VDS contains a rules database that contains rules that describe vulnerabilities and provide a programmatic means to check for the presence of those vulnerabilities. In particular, the information received from a network as a result of reflex testing is checked against the rules database and can be used to detect every device in the network, identify each host's operating system as well as the open ports of the host and the applications being run on them. This information is then used to identify vulnerabilities. An intrusion detection system (IDS) examines network traffic for signs of malicious activity. The rules used by the IDS are determined by the VDS vulnerability analysis, so that only rules that describe possible intrusion conditions as they exist for the specific network are loaded. Such a Target-based IDS monitors for specific conditions to which the network has been determined to be vulnerable, as well as any range of conditions or attacks to which the network might be vulnerable.
>
> However, Flowers fail to teach: "identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors; based on a

C

ForcePoint LLC
EX-1002
Page623

> packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type", i.e., Flowers teaches monitoring for attacks based on vulnerabilities identified in the network but does not teach identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.
>
> None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

In response, applicant respectfully points out that features of at least some of the independent claims (e.g., 21, 26, 31, and 60) are not necessarily the same as those the Examiner has highlighted above. For example, Claim 26 includes "permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices," in the context claimed.

As additional, non-exhaustive examples, Claims 21, 26, 31, and 60 recite the following, respectively:

C

ForcePoint LLC
EX-1002
Page624

21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors;

based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

C

ForcePoint LLC
EX-1002
Page625

wherein the at least one configuration involves at least one operating system.

26. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;

based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices

ForcePoint LLC
EX-1002
Page626

for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

31. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

display information that is based on the first vulnerability information;

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified

ForcePoint LLC
EX-1002
Page627

vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and

receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors;

wherein the at least one configuration involves at least one operating system.

60. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including:

at least one first potential vulnerability, and

at least one second potential vulnerability;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;

based on a packet analysis, determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

ForcePoint LLC
EX-1002
Page628

permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system.

Clearly, at least some of the independent claims are not necessarily limited to the features that the Examiner has noted in the Examiner's Statement of Reasons for Allowance, as noted above (by way of example only). Instead, each of the claims should only be limited by the language existing therein.

Further, although Applicant agrees with the Examiner's conclusion that these claims are allowable, Applicant notes that the claims may be allowable for reasons other than those identified by the Examiner and does not concede that the Examiner's characterizations of the terms of the claims and the prior art are correct. Each of the claims stands on its own merits and is patentable because of the combination it recites and not because of the presence or absence of any one particular element.

ForcePoint LLC
EX-1002
Page629

The Examiner's Statement was not prepared by Applicant and only contains the Examiner's possible positions in one or more reasons for allowability. Thus, any interpretation with respect to the Examiner's Statement of Reasons for Allowance should not be imputed to the Applicant.

Respectfully submitted,



Dated: 14 Feb 2020

Patrick E. Caldwell, Esq.
Reg. No. 44,580

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

C

ForcePoint LLC
EX-1002
Page630

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

92845 7590 01/15/2020
The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	05/30/2017	Brett M. Oliphant	SP1P012C	9647

TITLE OF INVENTION: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~SMALL~~ LARGE	~~$500~~ $1000	$0.00	$0.00	~~$500~~ $1000	04/15/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
HERZOG, MADHURI R	2438	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Patrick E. Caldwell, Esq.
2 The Caldwell Firm, LLC
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
SecurityProfiling, LLC	Garland, TX

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☒ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☒ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Patrick Caldwell/ Date 14 Feb 2020

Typed or printed name Patrick Caldwell Registration No. 44580

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

ForcePoint LLC
EX-1002
Page631

C

Electronic Patent Application Fee Transmittal

Application Number:	15608978
Filing Date:	30-May-2017
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012C

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt	
EFS ID:	38599635
Application Number:	15608978
International Application Number:	
Confirmation Number:	9647
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	92045
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012C
Receipt Date:	14-FEB-2020
Filing Date:	30-MAY-2017
Time Stamp:	23:41:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	E20202DN42059910
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Post Allowance Communication - Incoming	SP1P012C_Comments_vF_14-Feb-2020.pdf	144464 dcbbbbd78b2833b625bb7b710339d7f265fa756b	no	9
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	SP1P012C_fee-transmittal_vF_14-Feb-2020.pdf	130089 31ef02d34bcb3f1a35e6cfe63cd1ee17a6730e82	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30333 be66ecee1780a5aa85734c345b4daaa4f333c548	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	304886		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/608,978	03/31/2020	10609063	SP1P012C	9647

92045 7590 03/11/2020

The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Brett M. Oliphant, Plano, TX;
SecurityProfiling, LLC, Woodville, TX;
John P. Blignaut, West Lafayette, IN;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.