

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.
Petitioner

v.

WEBROOT INC.

Case No. IPR2023-00677
Patent No. 9,578,045

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 9,578,045**

Filed on behalf of Trend Micro, Inc.

By: Robert M. Hansen

Matthew J. Anderson

Scott B. Amankwatia

The Marbury Law Group, PLLC

11800 Sunrise Valley Drive

15th Floor

Reston, VA 20191

Tel: (703) 391-2900

Fax: (703) 391-2901

TABLE OF CONTENTS

I. Mandatory Notices (37 C.F.R. § 42.8(a)(1))	1
PAYMENT OF FEES:	3
II. Grounds for Standing (37 C.F.R. § 42.104(a))	3
III. Identification of Challenge (37 C.F.R. § 42.104(b))	4
A. Citation of Prior Art	4
B. Statutory Grounds for Challenge	4
IV. The '045 Patent	5
A. Claim of Priority of the '045 patent	5
B. Specification of the '045 Patent	5
C. Summary of the Prosecution History	6
D. Level of Ordinary Skill in the Art	8
E. Claim Construction	9
V. Grounds of Rejection	10
A. Ground 1: Claims 1-19 are unpatentable under 35 U.S.C. § 103 as obvious in view of Rockwood in view of Xie.	10
1. Claim 1	14
a. A method comprising:	14
b. gathering one or more events defining an action of a first object acting on a target;	14
c. generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;	17

d.	obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;	21
e.	assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and	26
f.	transmitting the assembled event line.	28
2.	Claim 2	28
a.	The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and	28
b.	wherein the event line is transmitted to an end recipient.	30
3.	Claim 3	30
	The method of claim 1, further comprising:.....	30
	obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.....	30
4.	Claim 4	32
	The method of claim 1, wherein the at least one event includes information uniquely identifying the object performing the action,	

information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.	32
5. Claim 5	34
 The method of claim 4, further comprising:.....	34
 a. determining whether a global perspective for the at least one event has been cached;	34
 b. when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and	35
 c. when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database.	36
6. Claim 6	38
 The method of claim 5, further comprising:.....	38
 a. determining whether the cached global perspective for the at least one event has expired; and	38
 b. when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.....	39
7. Claim 7	40
 The method of claim 4, further comprising:.....	40
 heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one	

	characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object...	40
8.	Claim 8	42
	a. A system for providing forensic visibility into a system, comprising:	
		42
	b. a device including:.....	42
	c. a communication interface;	42
	d. a processor;	43
	e. data storage; and	43
	f. a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:.....	43
	g. gather one or more events defining an action of a first object acting on a target;	44
	h. generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;	44
	i. obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator	

	(URL) information, wherein the global perspective for one or more related events to the at least one event across a network;	44
	j. assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and	45
	k. transmit the assembled event line utilizing the communication interface.	45
9.	Claim 9	45
	The system of claim 8, wherein the at least one of the one or more events is executed by the processor.	45
10.	Claim 10	46
	The system of claim 8, further comprising:	46
	a. a global perspective information server; and	46
	b. an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.	47
11.	Claim 11	48
	The system of claim 8, wherein the sensor agent is further operable to: cache the one or more events; and asynchronously consolidate and normalize the one or more events.	48
12.	Claim 12	49
	The system of claim 8, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and	

	information uniquely identifying the target upon which the act is being performed.	49
13.	Claim 13	50
	The system of claim 12, wherein the sensor agent is further operable to:	50
	a. determine whether the global perspective for the at least one event has been cached;	50
	b. when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and	50
	c. when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database.....	51
14.	Claim 14	51
	The system of claim 13, wherein the sensor agent is further operable to:	51
	a. determine whether the cached global perspective for the at least one event has expired; and	51
	b. when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database.....	52
15.	Claim 15	52
	The system of claim 12, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a	

	location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.....	52
16.	Claim 16	53
	a. A system for providing forensic visibility into a system, comprising:.....	53
	b. a device including:.....	53
	c. a communication interface;	53
	d. a processor;	54
	e. data storage; and	54
	f. a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:.....	54
	g. gather one or more events defining an action of a first object acting on a target;	54
	h. generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;	55
	i. assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and.....	55

j.	transmit the assembled event line utilizing the communication interface.....	56
17.	Claim 17	56
	The system of claim 16, further comprising a global perspective information server including:	56
a.	a processor;	56
b.	a communication interface;.....	57
c.	data storage; and	57
d.	a global perspective module, wherein the global perspective module is operable to:	57
e.	receive the event line from the device;.....	57
f.	obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information;	58
g.	assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and.....	58
h.	transmit the assembled second event line utilizing the communication interface to an end recipient.	61
18.	Claim 18	62
	The system of claim 17, wherein the end recipient heuristically displays information identifying the first object performing the	

	action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.	62
19.	Claim 19	63
	a. The system of claim 16, further comprising a bridge including:..	63
	b. a processor;	63
	c. a communication interface;	63
	d. a cached event store, wherein the cached event store is operable to:	63
	e. receive a first request for a global perspective for the at least one event;.....	64
	f. receive a second request for a global perspective for another event, the second request originating from another device;	64
	g. obtain a first global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information;	65
	h. obtain a second global perspective for the another event;.....	65
	i. provide the first global perspective to the device; and	66
	j. provide the second global perspective to the another device.....	66

VI. NO BASIS FOR DISCRETIONARY DENIAL	67
VII. CONCLUSION	69

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (Feb. 13, 2020).....	67
<i>Cellco Partnership v. Huawei Device Co.</i> , IPR2020-01117, Paper 10 (Feb. 3, 2021).....	68
<i>General Electric v. Vestas</i> , IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018).....	10
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	10
<i>KSR Int’l Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007)	10
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	9
<i>Western Digital Corporation v. Spex Technologies, Inc.</i> , IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018).....	9

Statutes

35 U.S.C. § 102(a)(1).....	4
----------------------------	---

Rules

37 C.F.R. § 42.10(a).....	2
37 C.F.R. § 42.104(a).....	3
37 C.F.R. § 42.8(a)(1)	13
37 C.F.R. § 42.8(b)(2).....	13
37 C.F.R. § 42.8(b)(3).....	2

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 9,578,045 to Jaroch <i>et al.</i>
1002	Expert Declaration of Dr. Seth Nielson
1003	CV of Seth Nielson
1004	U.S. Patent No. 7,352,280 to Rockwood, Troy
1005	Xie - A Spatiotemporal Event Correlation Approach to Computer Security
1006	Prosecution History of '045 Patent
1007	Peterson, et al., “Computer networks: a systems approach,” Morgan Kaufmann Publishers, Inc., 1996
1008	Bangia, <i>et al.</i>, “Operating Systems and Software Diagnostics” (2007).
1009	U.S. Published Patent Application No. 2013/0067576 to Niemela
1010	Hutchins, <i>et al.</i>, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, The Proceedings of the 6th International Conference on Information Warfare and Security, March 17-18, 2011.
1011	Cheswick, <i>et al.</i>, “Firewalls and Internet Security Second Edition, Repelling the Wily Hacker”, 2003.
1012	Anderson, “Network Attack and Defense”, Security Engineering Volume 2, 2008.
1013	Wilding <i>et al.</i>, Virus Bulletin, The Authoritative International Publication of Computer Virus Prevention Recognition and Removal, July 1989.
1014	Lardinois, Google Acquires Online Virus Malware and URL Scanner VirusTotal, TechCrunch, September 7, 2012.
1015	Lasser, “Special Focus Issue: Security”, ;login: The Magazine of USENIX & Sage, 51-54, (November 2001).

Trend Micro, Inc. (“Petitioner”) petitions for *inter partes* review (IPR) of claims 1-19 of U.S. Patent No. 9,578,045 to Jaroch *et al.*, entitled “METHOD AND APPARATUS FOR PROVIDING FORENSIC VISIBILITY INTO SYSTEMS AND NETWORKS” (“the ’045 patent,” EX1001), which according to PTO records, is assigned to Webroot, Inc.

I. Mandatory Notices (37 C.F.R. § 42.8(a)(1))

REAL PARTY IN INTEREST:

The real parties-in-interest are Trend Micro, Inc., Trend Micro America, Inc., and Trend Micro, Incorporated. Trend Micro, Inc. is a wholly owned subsidiary of Trend Micro America, Inc., which is a wholly owned subsidiary of Trend Micro Incorporated, a Japanese Corporation.

RELATED MATTERS:

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner identifies the following related matters.

The ’045 patent is at issue in the following district court litigations:

- *Webroot, Inc. and Open Text, Inc. v. Trend Micro Inc.*, Case No. 6:22-cv-00239 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. Sophos LTD.*, Case No. 6:22-cv-00240 (W.D. Tex.), which was originally filed on March 4, 2022.

- *Webroot, Inc. and Open Text, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.*, Case No. 6:22-cv-00241 (W.D. Tex.), which was originally filed on March 4, 2022.
- *Webroot, Inc. and Open Text, Inc. v. AO Kaspersky Lab*, Case No. 6:22-cv-00243 (W.D. Tex.), which was originally filed on March 4, 2022.

Petitions for IPR of the '045 patent and U.S. Patent No. 10,257,224 ("the '224 patent"), a continuation of the '045 patent, have been filed:

- Petitioner filed an IPR petition for the '224 patent on March 3, 2023, Case No. IPR2023-00657.
- CrowdStrike, Inc. filed an IPR petition for the '045 on November 30, 2022, Case No. IPR2023-00124.
- CrowdStrike, Inc. filed an IPR petition for the '224 patent on October 31, 2022, Case No. IPR2023-00126.

LEAD AND BACKUP COUNSEL:

Pursuant to 37 C.F.R. § 42.8(b)(3) and 37 C.F.R. § 42.10(a), Petitioner appoints:

Robert M. Hansen (Reg. No. 43,656) as lead counsel, and
Scott B. Amankwatia (Reg. No. 78,226) as back-up counsel.
Matthew J. Anderson (Reg. No. 78,257) as back-up counsel.

Pursuant to 37 C.F.R. § 42.10(b), a power of attorney is being filed with this designation of counsel.

SERVICE INFORMATION:

Petitioner provides the following service information for designated counsel:

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: (703)-391-2900
Fax: (703)-391-2900

Petitioner consents to electronic service by email to the email addresses:

rhansen@marburylaw.com;
samankwatia@marburylaw.com;
manderson@marburylaw.com; and
pat-docketing@marburylaw.com.

PAYMENT OF FEES:

The PTO is authorized to charge any fees due during this proceeding to Deposit Account No. 18-1579.

II. Grounds for Standing (37 C.F.R. § 42.104(a))

Petitioner certifies that the '045 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in this Petition.

III. Identification of Challenge (37 C.F.R. § 42.104(b))

A. Citation of Prior Art

Petitioner cites the following prior art references:

U.S. Patent 7,352,280 to Rockwood, Troy (“Rockwood” EX1004) is prior art at least under AIA § 102(a)(1) because it published on April 1, 2008, more than one year before the earliest priority date of the ’045 patent. Rockwood was not submitted to or considered by the USPTO during prosecution of the ’045 patent.

Xie, Yinglian. “A Spatiotemporal Event Correlation Approach to Computer Security” Thesis. (August 2005) Carnegie Mellon University, Pittsburgh, PA.

(“Xie” EX1005)¹ is prior art under AIA 35 U.S.C. § 102(a)(1) because it was published by ProQuest in 2009, more than 1 year before the earliest priority date of the ’045 patent. EX1005 at pp.149-152. Xie was not submitted to or considered by the USPTO during prosecution of the ’045 patent.

B. Statutory Grounds for Challenge

Petitioner requests review of claims 1-19 on the following ground:

GROUND 1: Claims 1-19 are unpatentable under 35 U.S.C. § 103 as obvious in view of Rockwood (EX1004) and Xie (EX1005).

¹ Xie citations are to the Bates numbers, not the printed page numbers.

IV. The '045 Patent

A. Claim of Priority of the '045 patent

The '045 patent issued on February 21, 2017, from U.S. Patent Application No. 14/270,069, filed May 5, 2014. This application claimed priority to a provisional application 61/819,470, filed on May 3, 2013.² EX1001, Cover.

B. Specification of the '045 Patent

The '045 patent describes methods, and systems performing the methods, for allegedly providing forensic visibility into systems and networks. EX1001, p.1. Sensors may receive events defining actions of objects acting on targets, and the event, objects and targets may be correlated to an originating object to create an audit trail for each event. *Id.* A global perspective indicating age, popularity, malware classification, and address information may be obtained and associated with at least one of the event, target, or object; then an event line containing the event information may be assembled and transmitted for display to an end user. *Id.*, 25:29-52.

² Petitioner does not concede that the provisional application filing date of May 3, 2013, is the earliest priority date for any claim of the '045 patent. However, the priority date is not at issue in this Petition as Rockwood and Xie are prior art under 35 U.S.C. § 102(a)(1).

Claims 1-7 recite methods, and claims 8-15 recite a system including a device comprising a communication interface, a processor, and data storage, and a sensor agent that performs those methods. Specifically, claim 1 recites: “gathering one or more events defining an action of a first object acting on a target; generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object; obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network; assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line.” *Id.*, 25:28-52, 26:26-61. The dependent claims recite further limitations regarding method

elements and displaying information regarding the objects, actions and the global perspective. *Id.*, 25:53-26:28, 26:63-27:40.

Claims 16-19 recite a system for providing forensic visibility into a system comprising a device including a communication interface, a processor, and data storage, and a sensor agent in the data store executable by the processor to perform to “gather one or more events defining an action of a first object acting on a target; generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object; assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and transmit the assembled event line utilizing the communication interface.” *Id.* 27:41-28:4. Dependent claims 17 and 18 add a global perspective information server to the system, dependent claim 19 adds a bridge for communicating global perspectives to devices. *Id.* 28:5-62.

C. Summary of the Prosecution History

The Office issued a non-final rejection September 16, 2015 citing U.S. Pub. 2013/0298244 to Kumar et al. and rejecting various claims under 35 U.S.C. §112 and 35 U.S.C. §101, while finding only claim 20 allowable. EX1006, pp.97-102. Webroot responded with minor amendments and arguments on *Id.*, pp.71-92. A Final Rejection then issued May 31, 2016. *Id.*, pp.55-65.

An After-Final Response was filed in reply. *Id.*, pp.42-54. The After-Final Response added the limitation “wherein the global perspective for one or more related events to the at least one event across a network” [sic] to the independent claims.

A Notice of Allowance (NOA) issued October 5, 2016, in which a minor Examiner’s Amendment corrected a dependent claim. EX1006, pp.18-25. No Reasons for Allowance were included in the NOA. *Id.*

D. Level of Ordinary Skill in the Art

As established by the Declaration of Dr. Seth Nielson dated March 6, 2023 (EX1002), a person having ordinary skill in the art (“PHOSITA”) at the time of the earliest claimed priority date for the ’045 patent would have had a bachelor’s degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics such as malware/exploit

detection and/or network forensics. More education can supplement practical experience and vice versa. EX1002, ¶96.

E. Claim Construction

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. §42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

In parallel litigation, Webroot argues all claim terms should be given their plain and ordinary meanings, except for “wherein the global perspective for one or more related events to the at least one event across a network,” which Webroot contends should be construed as “wherein the global perspective is for one or more related events to the at least one event across other devices on a network.” For purposes of this proceeding only, Petitioner proposes the Board adopt Webroot’s proposals. See *Western Digital Corporation v. Spex Technologies, Inc.*, IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018) (finding Petition based on claim constructions urged by Patent Owner satisfies the claim construction requirements and Petitioner is not required to express its subjective agreement regarding correctness of the proffered claim construction or take ownership of the

construction); *see also General Electric v. Vestas*, IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018).³

V. Grounds of Rejection

The following discussion and the accompanying evidence demonstrate that there is a reasonable likelihood that Petitioner will prevail with respect to the challenged claims.

A. Ground 1: Claims 1-19 are unpatentable under 35 U.S.C. § 103 as obvious in view of Rockwood (EX1004) in view of Xie (EX1005).

Petitioner evaluates the scope and content of the prior art, any differences between the art and the claims, and the knowledge of person of ordinary skill in the art in accordance with *Graham v. John Deere Co.*, 383 U.S. 1 (1966) and *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007). Petitioner is unaware of any secondary considerations relevant to the '045 patent and a more than adequate written rationale is provided to support the combination of Rockwood and Xie under *KSR*.

Rockwood discloses a system that uses collected network data to identify attributes of events that may be intrusions in a network. EX1004, 5:60-67; EX1002, ¶¶100-102. These detected events on the network are correlated by a

³ Petitioner reserves the right in other proceedings to construe the Challenged Claims and pursue indefiniteness theories.

correlation engine based on attributes such as source IP, destination IP address, the operating system (OS) of the source, the timing of the event, and other attributes.

EX1004, 11:4-20,12:1-35; EX1002, ¶¶98-99. These detected events are correlated based on shared attributes to identify an attack, a target event (ruleset characterizing an attack), and an attacker. EX1004, 5:17-20,13:1-65; EX1002, ¶¶104-105,109-110,123. Rockwood places these correlated attributes into an abstracted n-dimensional graph to provide a global view of a detected event and related events. EX1004, 8:6-12,14:1-35; EX1002, ¶¶103,107,124.

In the same field of endeavor, Xie improves on existing correlation methods for event detection in networks to reduce false positives and provide a broader view of attacks. EX1005, pp.19, 32-33; EX1002, ¶¶126,128,131. In particular, Xie teaches expanding the correlation space of network events to include event detection in files on computers of the network. EX1002, ¶¶114-116,127,131; Xie uses this broader event data to not only reduce false positives but also more clearly identify the files associated with malware on a device (e.g., originating malware that is the source of an attack). EX1005, pp.61-65; EX1002, ¶¶130,132-135.

Motivation to Combine Rockwood and Xie

Rockwood discloses a system that uses collected network data to identify attributes of events that may be intrusions in a network. EX1004, 5:60-67; EX1002, ¶¶99-102. These detected events on the network are correlated by a

correlation engine based on attributes such as source IP, destination IP address, the operating system (OS) of the source, the timing of the event, and other attributes.

EX1004, 11:4-20,12:1-35; EX1002, ¶¶101-102. These detected events are correlated based on shared attributes to identify an attack, a target event (ruleset characterizing an attack), and an attacker. EX1004, 5:17-20,13:1-65; EX1002, ¶¶99-100,118-120. Rockwood correlates and compares stored (previously analyzed) events to identify which event(s) is closest to the target event in the conceptual n-dimensional space. EX1004, 1:36-56, 6:63-7:16; EX1002, ¶¶100-102,120-121.

In the same field of endeavor, Xie improves on existing correlation methods for event detection in networks to reduce false positives and provide a broader view of attacks. EX1005, pp.19, 32-33; EX1002, ¶¶122-124,130. In particular, Xie teaches expanding the correlation space of network events to include event detection in files on computers of the network. EX1002, ¶¶109-115,132-137; Xie uses this broader event data to not only reduce false positives but also more clearly identify the files associated with malware on a device (e.g., originating malware that is the source of an attack). EX1005, pp.61-65; EX1002, ¶¶122-135.

A PHOSITA would have been motivated to combine the teachings of Rockwood and Xie to improve intrusion event detection, which is the focus of both prior art references. EX1002, ¶¶122,132-137. A PHOSITA as of the '045 priority

date would have looked to Xie to improve the system of Rockwood by applying the added detection capability provided by expanding the correlation space of network events to include event detection in files on computers of the network to improve identification of the sources or origin points of a network attack traffic detected by Rockwood. EX1005, pp.21,26,61; EX1002, ¶¶109-115,132-137. Thus, the correlation of events in Rockwood to attacks and attackers would be expanded by Xie to include correlation of the events to malware on the network when that is the source of the attack. EX1002, ¶¶132-137. In the modified system of Rockwood-Xie, the events are correlated to attacker profiles to help identify the source of an attack (attacker or originating malicious file as the case may be). EX1002, ¶¶132-137.

Further, a PHOSITA would have looked to Xie to improve the global view of events on a network being monitored by the system of Rockwood by adding the file event detection and correlation capability described in Xie. EX1005, pp.61,63; EX1002, ¶¶132-137. A PHOSITA would have recognized that the systems of Rockwood and Xie are complementary in their event detection and are predictably combinable in the correlation, analysis, and presentation processes. EX1005, pp.26-27,32-33,66-68,124,128; EX1004, 3:50-67,4:25-35,10:45-60; EX1002, ¶¶132-137. Being complementary, a PHOSITA would have known there was a

high likelihood of success in combining Rockwood and Xie. *Id.* The analysis for this section is incorporated by reference into each subsection/limitation below.

1. Claim 1

a. A method comprising:

Both Rockwood and Xie disclose methods in the form of computing processes that use event detection in computer networks to identify malware.

EX1002, ¶141; EX1004, 1:35-55; EX1005, pp.29,35.

b. gathering one or more events defining an action of a first object acting on a target;

Rockwood discloses detecting and collecting information regarding actions and activity on a network. EX1004, 20:35-45; EX1002, ¶143-148. Rockwood discloses the terms recited in this claim element in two ways that the disclosure in Rockwood can be mapped to this claim limitation.

In a first mapping, Rockwood discloses detecting and recording characteristics of a network event (corresponding to “gathering one or more events defining...”) including a source IP address (and its OS) of an event and a destination IP address (corresponding to “target”) for sent data (corresponding to “action...”). EX1004, 5:60-6:65,13:45-65; EX1002, ¶149-151. Further, the device, operating as the source of the event and corresponding to the source IP address or source port, transmits data (of an event) via the network layer / its operating system (OS) (corresponding to “first object”), which the system of Rockwood records in a

detected event. EX1004, 6:25-35,10:15-20,12:25-55; EX1002, ¶149-153.

Specifically, Rockwood states:

These packets and similar network communications received by sensors 20 are referred to as detected events 110. The data that makes up detected events 110 is referred to as event information. A detected event 110 may be an attack...

EX1004, 3:37-41.

Each detected event 110 comprises a plurality of characteristics such as, for example, time, source IP address, and destination IP address. These characteristics are referred to as attributes 410...

Id., 5:63-66.

System 10 detects this attack as detected event 110f, which occurred at 5:20 p.m. and originated from a UNIX-based computer. Detected event 110f contains a segment of code signifying that detected event 110f is an attack.

Id., 12:39-44.

Thus, Rockwood discloses gathering the event and attributes corresponding to the event. EX1004, 3:36-43,5:60-6:65,13:45-65; EX1002, ¶152. These attributes include the operating system (e.g., UNIX) transmitting data (of an event) and the destination (“target”) as well as code/data transmitted from the network layer / OS to the target (“action of a first object acting on a target”). EX1004, 10:15-20,12:35-45; EX1002, ¶149-155. A PHOSITA would have understood that the network

layer/OS (“first object”) executes on a device (e.g., the device at the source IP).

EX1002, ¶63-85,143-152 (citing exhibits EX1007-EX1015).

In a second mapping, Rockwood also discloses detecting and recording characteristics of an event (corresponding to “gathering one or more events defining...”), including a transmitting source of an event and a destination IP address (corresponding to “target”) where the data/code package (corresponding to “first object”) is transmitted. EX1004, 5:60-6:65,12:35-45,13:45-65; EX1002, ¶153-160. Rockwood notes that the data package includes executable code (corresponding to “first object”) that may be malware; and, therefore, event attributes relating to the package (e.g., malware) transmission and its effect/action on a target (corresponding to “events defining an action of the first object...”) are collected by the system of Rockwood. EX1004, 3:50-60,12:35-45; EX1002, ¶¶153-160. This executable code is transmitted to the destination device or intermediate node to execute on that device (corresponding to “the first object is executed on a device”). EX1004, 3:50-60,12:35-45; EX1002, ¶¶157-159.

Either of these ways in which Rockwood discloses the recited claim language demonstrates that Rockwood renders this limitation obvious. EX1002, ¶¶149-161.

- c. generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;**

The '045 patent describes that the contextual state may include “originating processes, devices, and users” and may include “more or less information and in varying combinations.” EX1001, 8:40-45,17:35-40; EX1002, ¶166. Rockwood and Xie disclose using an attacker profile to correlate an event to an originating object/process of the first object (e.g., originating malware or source) of an attack that causes a network layer / OS (“first object”) to transmit data such as an attack/malware (e.g., copy of the originating malware)), wherein such correlated data (corresponding to “contextual state”) includes information such as originating processes/objects, devices, and users (as discussed below). EX1002, ¶¶166-170; EX1004, 2:60-3:5,6:1-62,13:1-24.

In the first mapping of the network layer/OS in Rockwood to the “first object,” Rockwood discloses a correlation engine that correlates detected events (e.g., attacks) from a source (e.g., OS such as UNIX with network layer, or source IP address) with source of the attack, embodied as an attacker profile or originating malware (“originating object”). EX1002, ¶¶166-171; EX1004, 7:60-8:5,11:4-44,12:36-55. A PHOSITA would have recognized that the sources of attacks or originating malware (corresponding to “originating object of the first object”)

corresponding to detected events would be generating events/attacks to be transmitted via the network layer/OS (“first object”). EX1002, ¶¶169-171; EX1004, 12:36-55,12:20-67,24:40-50. Thus, a PHOSITA would have understood that Rockwood’s teachings of correlating events to sources of attacks using attacker profiles (which includes information relating to a device on which the first object (network layer/OS) is executed and a user associated with the first object) and attack attributes (e.g., target events) discloses “generating a contextual state.” EX1002, ¶¶174-177.

Further, Xie discloses identifying the identity/name and location of the originating malware (e.g., Lion worm) based on correlations of network events and file events on the network (e.g., file changes in network devices that indicate presence of an attack and its source (originating malware)). EX1005, pp.30-32,47-49; EX1002, ¶¶179-181. That is, Xie teaches identifying originating malware of an attack (“originating object”) (e.g., that causes a network layer / OS (“first object”) to transmit malware), based on correlated events and connecting those events to the code and affected files constituting the malware within the OS (e.g., Linux/Windows) and its source (originating malware). *Id.* As described in the motivation to combine above, the combined Rockwood-Xie analyzes network attacks using network events and file events together to correlate event information to an attack and its source (e.g., attacker or originating malware), and modifies

Rockwood's attacker profiles to include the identified originating malware information (as disclosed by Xie). EX1002, ¶118-138. Accordingly, a PHOSITA would have understood that Rockwood-Xie teaches "for at least one of the one or more events by correlating the at least one event to an originating object." EX1002, ¶¶177-184.

In the second mapping of the data package (e.g., transmitted malware) as the "first object," Rockwood and Xie disclose this limitation for the same reasons above. EX1002, ¶¶171-173. The above-discussed source of attack/originating object is the originating malware ("originating object") and would remain so in the second mapping where the transmitted malware is the claimed first object. EX1002, ¶¶171-173. Thus, the above-discussed process of correlating an event to an originating object (e.g., attacker profile with originating malware information as in Xie) that provides "contextual state" also applies to the above-referenced second mapping and discloses this limitation. EX1002, ¶173.

Further regarding the contents of the contextual state, under the first mapping, Rockwood-Xie discloses the network layer/OS executing on a device as the "first object," and therefore, this device (e.g., a device of an attacker) corresponds to "contextual state including...an indication of...a device on which the first object executed." EX1002, ¶170-173, 187-191; EX1004, 10:8-22. Under the second mapping, the transmitted data package ("first object") executes on a

device such as a destination device (identified by its IP address, which is included in event information and contextual state). *Id.*

Further, Rockwood-Xie discloses correlating the event/attack with an attacker profile, which includes information concerning an individual carrying out the attack (corresponding to “contextual state including...an indication of...a user associated with the first object” under either mapping). EX1002, ¶170-173,187-191; EX1004, 10:8-22.

Under either mapping, Rockwood and Xie disclose associating an event (containing the data package (“first object” under the second mapping)) with a source behind an attack / attacker profile (e.g., originating malware/object) that caused a network layer/OS (“first object” under the first mapping) to transmit the data, to generate contextual state and thus disclose “the contextual state including an indication of the originating object of the first object.” EX1002, ¶170-173,187-190; EX1004, 6:25-35,7:20-25,8:6-65,13:1-25,15:65-16:7.

A PHOSITA would have been motivated to include the file change correlations of Xie with the correlations of Rockwood and include Xie’s originating malware information in Rockwood’s attacker profile to achieve the benefits of increased accuracy and more specific containment information. EX1005, pp.61,63; EX1002, ¶¶118-138.

Thus, Rockwood in view of Xie renders this limitation obvious. EX1002,

¶¶166-185.

- d. obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;**

As described regarding limitation 1[c] above, Rockwood correlates the event to sources and corresponding attacker profiles (as modified by Xie) to provide a context/contextual state for an event. EX1002, ¶¶166-187,200. Further, Rockwood discloses correlating the event to other events and attributes across the network to generate a global view of an attack using attacker profiles (as modified by Xie) (corresponding to “obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object”). EX1004, 14:24-29,19:27-31; EX1002, ¶¶196-199. The Rockwood-Xie combination discloses attributes forming their global view that are similar to those attributes stated as being part of the global perspective in the ’045 patent disclosure. EX1002, ¶¶196-199. Thus, a PHOSITA would have understood that the global view that gives an operator a view into more events related to the event that was correlated to an attacker profile or attack teaches the limitation of “obtaining a global perspective for the at least one event by obtaining information

associated with one or more of the first object and the originating object.” EX1002, ¶¶198,200,204. As described above regarding limitation 1[c], Rockwood-Xie teaches the contextual state information. EX1002, ¶186.

The remaining features of limitation 1[d] are taught by Rockwood according to both the first mapping and the second mapping of “first object” explained above. For example, the above-discussed correlated information that provides a “global perspective” includes information discussed below that pertain to the “first object” and/or “originating object.”

In the first mapping of the network layer/OS to the “first object,” Rockwood discloses collecting event information identifying the network layer/OS of the source (e.g., source IP address or source port and/or OS) (“first object”) and correlating with other events based on that network information (corresponding to “wherein the global perspective comprises information associated with one or more of the first object”). EX1002, ¶¶196-198; EX1004, 9:17-45,12:19-67,22:24-34.

In the second mapping of the data package in Rockwood to the “first object,” Rockwood discloses associating a particular event with other detected events and correlating with an attacker profile/source of an attack (as modified by Xie to include originating malware information) (“wherein the global perspective

comprises information associated with one or more of ...the originating object”).⁴

EX1002, ¶123-125,192,195; EX1004, 6:25-35,8:6-65,13:1-25. Likewise, as described above regarding claim limitation 1[b], the malware code of the data package (“first object”) of an event/attack is collected and associated with the event (corresponding to “wherein the global perspective comprises information associated with one or more of the first object”). EX1002, ¶196-201; EX1004, 6:30-35,7:20-25,15:65-16:7.

In general, Rockwood states:

Generally, correlation engine 140 determines identified detected events 222 by identifying detected events 110 in detected event storage 158 corresponding to points 360 that are within proximity limits 370 of target point 362. Correlation engine 140 then correlates identified detected events 222 with one or more existing attacker profiles 224a in profile set 156. In particular, correlation engine 140 may identify the particular existing attacker profile 224a in profile set 156 that most closely matches identified detected events 222. Global server 40 sends the identified existing attacker profile 224a to console 50 as identified attacker profile 230. GUI 52 displays identified attacker profile 230 to operator 60. Operator 60 thus learns the likely identity of the individual or organization that caused identified detected events 222.

EX1004, 10:30-45.

⁴ This also applies to the first mapping above, so this element is disclosed by Rockwood under the first mapping for the same reason.

Thus, Rockwood provides a broader/global view into multiple events related to the selected event in a network using the correlations to the attacker profile. EX1002, ¶¶205-211; EX1004, 3:36-43,4:49-58,10:30-45. Based on either mapping, a PHOSITA would have understood that the network-level aggregation and global view of events across a network (comprising multiple devices) in Rockwood based on the correlated data as modified by Xie teach obtaining the recited global perspective “a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object,” as well as “wherein the global perspective for one or more related events to the at least one event across a network [sic]” / “wherein the global perspective is for one or more related events to the at least one event across other devices on a network” (see Section IV.E). EX1002, ¶¶196-211; EX1004, 4:5-55,15:34-44.

Regarding the “information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information,” Rockwood discloses aggregating a variety of information into a global view of network events that relate an event to other events on the network based on attacker profiles (as modified by Xie)

(corresponding to “global perspective”). EX1004, 4:5-55,15:34-44; EX1002, ¶198,204.

In the first mapping of the OS in Rockwood to the “first object,” Rockwood-Xie discloses obtaining event information related to the event timestamp (“age”), the OS (“first object”) of the source device, its IP address (“IP address”), similar correlated events (corresponding to “popularity”), and source of an attack (e.g., originating malware such as Lion worm) (corresponding to “a determination as to whether the originating object is malware”). EX1002, ¶¶196-205; EX1004, 6:25-35,8:6-65,10:1-25,12:19-55,24:40-50; EX1005, pp.47-49.

In the second mapping of the data package (that can be malware) in Rockwood to the “first object,” Rockwood-Xie discloses obtaining event information related to the IP addresses (corresponding to “IP address”) of source/destination devices, a timestamp (corresponding to “age”), similar correlated events (corresponding to “popularity”), a corresponding target event if the event is malware (corresponding to “a determination as to whether the first object is malware”), and the above-discussed originating malware (“a determination as to whether the originating object is malware”). *Id.* A PHOSITA would have understood that the network level aggregation and correlation of events in Rockwood-Xie and the cited information elements above teach the global

perspective that comprises at least one of the listed elements of this claim

limitation. EX1002, ¶¶196-205; EX1004, 4:5-55,15:34-44.

Therefore, the Rockwood-Xie combination discloses this limitation.

EX1002, ¶¶194-212.

- e. assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and**

Rockwood discloses collecting and combining information about events, including attacker profile information, that is subsequently displayed in a Graphical User Interface (GUI). EX1004, 10:34-44; EX1002, ¶¶216-219. The information related to events that is displayed in a GUI discloses “an event line including details associated with the at least one event.” EX1002, ¶219. As explained above regarding limitations 1[c] and 1[d], the displayed information (“event line”) is also related to collected events and the associated attacker profile that is or is part of both contextual state and the global perspective. This is consistent with the specification of the ’045 Patent. EX1002, ¶216, EX1001, 9:60-65,17:60-63. For example, Rockwood discloses displaying the attacker profile (“originating object”) on the GUI in connection with detected events and relevant details for each associated event such as information related to suspected attack and timestamp. EX1002, ¶¶216-218; EX1004 at 5:48-51,7:3-10,7:20-22,10:34-44,16:62-66. Thus, Rockwood displays event lines comprising information

relating to the event. A PHOSITA would have understood that because the data corresponding to event line is displayed in GUI, it is generated/assembled.

EX1002, ¶¶216-219.

Rockwood and Xie also disclose “the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object” for the reasons discussed above regarding limitations 1[b] and 1[c]. For example, Rockwood-Xie’s event information and/or correlated attacker profiles (that are part of the above-discussed “event line”) include information relating to the “first object” (e.g., network layer/OS of a source device identified by OS information or IP address, or transmitted malware), “action of the first object” (e.g., data transmission from source to target, or transmitted malware’s actions on a target), “target” (e.g., target device and its IP address), and the “originating object” (e.g., source of an attack or originating malware in attacker profiles). EX1002, ¶¶221-225; EX1004, 3:40-46,5:51-53,16:62-66.

A PHOSITA would have been motivated to combine Rockwood and Xie and configure Rockwood-Xie to include information discussed above in an event line to be displayed in the GUI to provide these details to the operator in order to provide information related to the event including the source of the attack in order to better clean up the network. EX1002, ¶¶118-138,223-224. A PHOSITA would have recognized that Xie’s information on the originating malware has a similar

purpose to Rockwood's attacker profiles, and thus would have been motivated to combine them to be included in the event line to be displayed in the GUI. *Id.*

Therefore, Rockwood in view of Xie discloses this limitation. *Id.* at ¶¶214-226.

f. transmitting the assembled event line.

Rockwood and Xie discloses this limitation. For example, as discussed above for limitation 1[e], Rockwood-Xie's event line is displayed in a GUI, so it is transmitted. EX1002, ¶228. Further, Rockwood discloses transmitting event line from one device to another (with the GUI), via network (e.g., via a secure shell tunnel). EX1004, 5:27-59, 18:6-65, FIG.1; EX1002, ¶228. Therefore, Rockwood in view of Xie discloses this limitation. *Id.* at ¶¶228-231.

For the foregoing reasons, a PHOSITA as of the earliest possible priority date would have found claim 1 of the '045 patent to be obvious in view of the combination of the teachings in Rockwood and Xie. EX1002, ¶¶139-231.

Accordingly, claim 1 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

2. Claim 2

a. The method of claim 1, wherein the information associated with the one or more of the first object and the originating object is obtained from a community database; and

Rockwood discloses providing a target event that is selected or defined by the operator and corresponds to malicious attacks, where the target events include

“one or more attributes 410 such as, for example, time, source IP address, and destination IP address.” EX1002, ¶234; EX1004, 7:5-8,10:1-58,24:40-50.

Rockwood also teaches a database of attacker profiles (which as discussed for Claim 1 relates to the “originating object”) defining characteristics of attacks. EX1002, ¶¶235-236; EX1004, 10:20-35. Further, Xie discloses that malware profile information (e.g., information relating to the originating object/malware such as worms) could be obtained from Internet-wide community sources, such as public websites from defensive organizations (corresponding to “community database”). EX1005, pp.46-47; EX1002, ¶236.

A PHOSITA would have been motivated to combine Rockwood and Xie. Based on Xie, a PHOSITA would have known to look to public websites for malware descriptions (relating to information on the originating malware/originating object, which (as discussed above for Claim 1) can be included in Rockwood’s attacker profiles) in analysis of network events. EX1002, ¶237. A PHOSITA would have recognized the value in having attacker profiles in combination with other malware profile information generated by public sources, because this would have reduced the amount of time required to build out the Rockwood system and incorporated knowledge from a wider range of experts in the field. *Id.*

Accordingly, the combination of Rockwood and Xie discloses this claim limitation. EX1002, ¶¶234-238.

b. wherein the event line is transmitted to an end recipient.

As discussed above for limitation 1[f], Rockwood discloses transmitting an event line (via a secure shell tunnel) from one device to another device (with a display/GUI) (corresponding to “end recipient”). EX1004, 5:27-59,22:24-45; EX1002, ¶¶228-230,240-242.

Therefore, a PHOSITA would have found the limitations recited in claim 2 obvious in view of the Rockwood-Xie combination. EX1002, ¶¶232-242. As shown, the Rockwood-Xie combination discloses all elements recited in claim 1 from which claim 2 depends. Accordingly, claim 2 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

3. Claim 3

The method of claim 1, further comprising:

obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event.

Rockwood discloses prioritizing a detected attack event based on event information. EX1004, 5:45-58,21:22-61; EX1002, ¶245. Rockwood explicitly teaches receiving severity levels (corresponding to “event priority”) for a cluster of related events collected from the network. EX1004, 19:37-40,21:20-60; EX1002, ¶¶245-246.

For example, Rockwood discloses basing the severity on various factors including proximity of an event to a particular network node which may host the malware (i.e., event information correlated to the originating object) (corresponding to “the generated context”).⁵ EX1004, 19:37-40,19:60-63,21:20-60; EX1002, ¶¶244-245. The severity discussed in Rockwood uses the relationship of the events to each other (similar to those discussed above in limitation 1[d] regarding “global perspective”) to determine “visibility” of an event in n-dimensional space. *Id.* Thus, the severity (event priority) is also based on the “global perspective” of the relationship between events. *Id.*

As Rockwood describes, this severity (like event line) is displayed to operator in the GUI. “[O]perator 60p is able to analyze the severity of a threat based on the severity of an alert.” Ex. 1004, 5:45-51,7:15-25,21:22-60; EX1002, ¶¶247-249. Because both the event line and event severity (priority) are displayed to an operator (in the GUI) and because both are related (e.g., relating to detected events), a PHOSITA would have been motivated to include the priority information in the event line (e.g., by changing the visibility of information forming the event line). *Id.* A PHOSITA would have understood that an operator would want to see the event priority, which is information relevant to the event,

⁵ Petitioner notes that “the generated context” in this claim has no antecedent basis.

along with relevant event information such as event line, in order to “analyze the severity of a threat based on the severity of an alert.” *Id.*, ¶¶244-249.

Therefore, a PHOSITA as of the earliest possible priority date would have found the limitations recited in claim 3 to be obvious based on Rockwood. *Id.*, ¶¶243-249. As shown, the Rockwood-Xie combination discloses all elements recited in claim 1 from which claim 3 depends. Accordingly, claim 3 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

4. Claim 4

The method of claim 1, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.

Rockwood discloses this claim for the reasons discussed above regarding claim limitations 1[b] and 1[e]. EX1004, 4:45-60; EX1002, ¶251.

In the first mapping of the network layer/OS to “the first object” in claim 1, Rockwood discloses recording the source IP address corresponding to the network layer (corresponding to “uniquely identifying the object”)⁶ of the originating device as a part of the detected event. EX1004, 4:45-60, 7:17-37; EX1002, ¶¶252-254. Further, Rockwood teaches recording information in packet headers and

⁶ Petitioner notes that “the object” in this claim has no antecedent basis.

payloads sent (corresponding to “uniquely identifying the action being performed”) by the network layer, and recording the destination IP address (“uniquely identifying the target upon which the act is being performed”) of the packet. EX1004, 7:15-39; EX1002, ¶251-256. A PHOSITA would have understood these collected attributes can be used to identify the object performing the action, the action, and the target in an event. EX1004, 4:45-60, 11:1-65; EX1002, ¶¶251-256.

In the second mapping of the data package in Rockwood to the “first object,” Rockwood discloses collecting event attributes including a source IP address, a packet (“uniquely identifying the object”) sent by the source device with its transmission details (corresponding to “uniquely identifying the action being performed”) such as timestamp, and the destination IP address (“uniquely identifying the target”). EX1004, 7:17-25; EX1002, ¶257. A PHOSITA would have understood these collected attributes can identify the object performing the action, the action, and the target in an event. EX1004, 6:10-27, 11:1-65; EX1002, ¶¶251-257.

Therefore, a PHOSITA would have found the limitations recited in claim 4 to be obvious based on Rockwood. EX1002, ¶¶250-258. As shown, the Rockwood-Xie combination discloses all elements recited in claim 1 from which claim 4 depends. Accordingly, claim 4 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

5. Claim 5

The method of claim 4, further comprising:

- a. determining whether a global perspective for the at least one event has been cached;**

Rockwood and Xie both teach storing event information from across a network (corresponding to “global perspective”) related to an event as described above regarding claim 1[d]. EX1005, pp.29-38,64; EX1004, 18:16-43; EX1002, ¶¶261,263. Rockwood discloses storing detected events in a memory module that is accessible by the correlating engine in an n-dimensional graph framework (corresponding to “global perspective...has been cached”). EX1004, 5:1-15; EX1002, ¶¶261-262.

Xie teaches reporting and caching file change events from across a network to a central database (corresponding to “a global perspective for the at least one event has been cached”). EX1005, pp.32-35; EX1002, ¶¶262-265. Xie discloses that the file update reports for retention and periodic retrieval are organized according to time/date and may be checked for successful upload/caching (corresponding to “determining whether...”). EX1005, pp.32-35; EX1002, ¶¶265-266. A PHOSITA would have been motivated to incorporate Xie’s caching technique (e.g., file change log of Xie), for example, to improve the storage efficiency of the memory module of Rockwood as described in Xie. EX1002, ¶¶128-138,266-267; EX1005, pp.22-23. Therefore, a PHOSITA would have

understood that these features recited in Rockwood-Xie are a disclosure of this limitation. EX1002, ¶261-268.

b. when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and

Xie discloses collecting and storing information on a daily basis related to file updates on hosts (e.g., connected computers) of the network (corresponding to “has been cached”). EX1005, pp.30-31; EX1002, ¶270. In other words, the network hosts transmit file updates that occurred since the last upload and this information is evaluated for malicious activity within that day. EX1005, pp.23-25; EX1002, ¶270. The next day the network hosts will likewise upload changes to files relative to the prior day. *Id.* A PHOSITA would have understood from this disclosure in Xie that after the file updates had been collected, correlated, and evaluated on a given day, the system would move on to the next day, and thus, the file update history has a one-day time to live, and the system determines if the TTL has been exceeded each day. EX1002, ¶¶270-271; EX1005, pp.26,35,40. Thus, each node gathers a “global perspective” on events happening on other nodes, all of which are pooled together to collectively represent the community’s “global perspective” of events happening on the network. EX1002, ¶¶270-271; EX1005, pp.40-41. As Xie explains, the cache (central database) uses such reports that are uploaded/cached. *Id.* Thus, Xie discloses this limitation. EX1002, ¶272.

A PHOSITA would have been motivated to use the caching techniques (including file storage process) of Xie to improve the storage efficiency of the memory module of Rockwood as described in Xie. EX1002, ¶¶267,270-271; EX1005, pp.22-23. A PHOSITA would have understood this improvement of Rockwood to work since the hosts of Rockwood already upload information and file update logging is well known in the art as described by Xie. *Id.* Therefore, a PHOSITA would have understood that that these features recited in Rockwood-Xie teach this limitation. EX1002, ¶¶270-272.

c. when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database.

Xie discloses that some uploads fail during periodic updates of file changes from the hosts of the network. EX1002, ¶274; EX1005, pp.24,40-41. That is, some file event information from hosts that represents a “global perspective” (as discussed above) on a given day may not be cached at the central server. *Id.* Nevertheless, Xie teaches that the file event/update information (representing a “global perspective” (for the reason discussed above)) sourced from the community of hosts other than the failed upload (corresponding to “community database”) is sufficient to make up for the missing information to give a global view of events needed for threat evaluation. EX1002, ¶¶274-277; EX1005, pp.22-23,35,40-41. Thus, a PHOSITA would have understood that Xie discloses “when

the global perspective for the event has not been cached, obtaining the global perspective for the at least one event from a community database.” *Id.*

A PHOSITA would have been motivated to incorporate Xie’s caching technique to Rockwood in order to source the global perspective of Rockwood from the community database in the event that the data was not on the memory module of Rockwood at least because the community data collected from the rest of the hosts provides an equivalent view. EX1002, ¶¶267,275-277. A PHOSITA would have understood this improvement of Rockwood to work since the hosts of Rockwood already upload information and the file update logging is well known in the art as described by Xie. EX1002, ¶¶277. Therefore, a PHOSITA would have understood that that these features recited in Rockwood-Xie teach this limitation. EX1002, ¶¶274-278.

For the foregoing reasons, a PHOSITA as of the earliest possible priority date would have found the limitations of claim 5 to be obvious based on the Rockwood-Xie combination. EX1002, ¶¶259-279. As shown, the Rockwood-Xie combination discloses all elements recited in claims 1 and 4 from which claim 5 depends. Accordingly, claim 5 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

6. Claim 6

The method of claim 5, further comprising:

- a. determining whether the cached global perspective for the at least one event has expired; and**

As discussed above regarding limitation 5[b], Xie discloses collecting and storing information related to file updates / events and correlations between them (representing a “global perspective”) on hosts of the network on a daily basis, and therefore a PHOSITA would have understood that after the file updates had been collected, correlated, and evaluated on a given day, the system would move on to the next day, such that file update history on a host expires after one day (having a time-to-live (TTL) value of one day). EX1002, ¶¶270-271,282; EX1005, pp.20-21,26,35,40-41. Thus, a PHOSITA would have understood that the system in Xie determines whether cached file updates (representing a “global perspective”) has expired each day. EX1002, ¶282.

Also as discussed above regarding limitation 5[b], a PHOSITA would have been motivated to use the file caching techniques (including storage process) of Xie to improve the storage efficiency of the memory module of Rockwood as described in Xie with an expectation of success because file update logging was well known in the art as described by Xie. EX1002, ¶¶270-271, 282; EX1005, pp.22-23. Therefore, a PHOSITA would have understood that Rockwood-Xie discloses this claim limitation. EX1002, ¶¶282-283.

b. when the global perspective for the at least one event has expired, obtaining a global perspective for the at least one event from a community database.

As described above regarding claim 5[c], Xie discloses that when an upload failure occurs, file event/update information associated with an event (representing “global perspective”) sourced from the community of hosts other than the failed upload (corresponding to “community database”) may be obtained and is sufficient to provide a global view needed to evaluate the threat event. EX1002, ¶¶274-277,285-287; EX1005, pp.22-23,35,40. Thus, Xie teaches that the aggregate view from the remaining hosts on the network constitutes a global view collected from a community, when data from a host is not uploaded or such data is past the day for file update logging (corresponding to “expired”), as would have been understood by a PHOSITA. *Id.* Also, as explained above, file event/update information is uploaded every day. Thus, when the information expires (after one day), new information (also representing global perspective) is uploaded/cached from the individual hosts (collectively the “community database”). EX1002, ¶¶274-287.

A PHOSITA would have been motivated to incorporate Xie’s caching technique to Rockwood for the reasons discussed above. EX1002, ¶¶118-138,267,287. A PHOSITA would have been motivated to source the global perspective of Rockwood from the community in the event that the data was not on the memory module of Rockwood, the reason being at least because the

community data collected from the rest of the hosts provides an equivalent view.

Id. A PHOSITA would have understood this improvement of Rockwood to be compatible and desirable since the hosts of Rockwood already upload information and the file update logging is well known in the art as described by Xie. EX1002, ¶267. Therefore, a PHOSITA would have understood that Rockwood-Xie discloses this claim limitation. EX1002, ¶¶288-289.

Therefore, a PHOSITA would have found the limitations of claim 6 to be obvious based on the Rockwood-Xie combination. *Id.*, ¶¶282-289. As shown, the Rockwood-Xie combination discloses all elements recited in claims 1, 4 and 5 from which claim 6 depends. Accordingly, claim 6 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

7. Claim 7

The method of claim 4, further comprising:

heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

The first portion of claim 7 recites heuristically displaying three types of information and the global perspective. The second portion of claim 7 recites a list

of elements such that the heuristic display is “according to one or more of” them.

These portions are addressed separately.

Rockwood discloses that information relevant to each network event is displayed in a selectable GUI. EX1004, 5:40-60,21:23-60; EX1002, ¶291-292. Less relevant (i.e., lower priority) information is hidden in the GUI to reduce clutter (corresponding to “heuristically displaying”) but is still available to a user. EX1002, ¶295. In the first mapping of the network layer of the OS in Rockwood to the “first object,” Rockwood discloses that the information displayed in the modifiable GUI (corresponding to “heuristically displaying”) includes the packets sent (corresponding to “identifying the action being performed”), a source IP address corresponding to the network layer (“first object”), destination IP address (“target”), and related events (corresponding to “global perspective”). EX1004, 5:40-60,7:1-65,8:5-20,10:8-22,12:36-67,16:62-66; EX1002, ¶¶291-295. In the second mapping of mapping the data package in Rockwood to the “first object,” the information displayed in the selectable GUI (“heuristically displaying”) includes the packet headers and payload (“first object”), source IP address, destination IP address (corresponding to “target”), and related events (corresponding to “global perspective”). EX1004, 5:40-60,7:1-65,8:5-20,12:36-67; EX1002, ¶¶291-296. An IP address represents a “location,” so Rockwood discloses

“heuristically displaying...according to...a location associated with the first object.” *Id.*

Therefore, a PHOSITA as of the earliest possible priority date would have found the limitations recited in claim 7 to be obvious based on Rockwood. EX1002, ¶¶290-297. As shown, the Rockwood-Xie combination discloses all elements recited in claims 1 and 4 from which claim 7 depends. Accordingly, claim 7 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

8. Claim 8

a. A system for providing forensic visibility into a system, comprising:

Rockwood discloses identifying the activities of an attacker through a correlation engine that collects detected events and compares them against “target” events that represent known or suspected attacks. EX1004, 6:60-7:15; EX1002, ¶298. Thus, Rockwood discloses the preamble.

b. a device including:

Rockwood teaches a manager server which may form a node of the network. EX1004, 4:5-39,14:24-30; EX1002, ¶¶303-304. Thus, Rockwood discloses this limitation.

c. a communication interface;

Rockwood teaches a GUI that opens a secure shell (SSH) tunnel to provide additional secure communications between a console and the other portions of

system including the manager server. EX1004, 4:5-39; EX1002, ¶304-306. Thus, Rockwood discloses this limitation.

d. a processor;

Rockwood teaches that the manager server is a computer or other processing device which has one or more processors. EX1004, 4:5-39; EX1002, ¶¶304,307.

Thus, Rockwood discloses this limitation.

e. data storage; and

Rockwood teaches detected event storage in a memory module. EX1004, 4:35-55; EX1002, ¶304,307. Thus, Rockwood discloses this limitation.

f. a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

Rockwood teaches a correlation engine connected or distributed across the manager servers, global server, and memory module. EX1004, 3:35-67,4:49-67; EX1002, ¶¶307-308. The correlation engine operates as an aggregator and interpreter of events and analyzes context of the events in relation to other events and attacker profiles, performing the processes recited by the remaining limitations. EX1004, 4:5-10,4:45-67,5:10-15; EX1002, ¶¶307-308. Thus, Rockwood discloses this limitation.

g. gather one or more events defining an action of a first object acting on a target;

Claim element 8[g] recites a limitation corresponding to the limitations recited in claim element 1[b]. As described above regarding claim 1[b], Rockwood teaches this limitation. EX1002, ¶¶143-161,298-299.

h. generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

Claim element 8[h] recites a limitation corresponding to the limitations recited in claim element 1[c]. As described above regarding claim 1[c], Rockwood in view of Xie teaches this limitation. EX1002, ¶¶163-192,298-299.

i. obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;

Claim element 8[i] recites a limitation corresponding to the limitations recited in claim element 1[d]. As described above regarding claim 1[d], Rockwood or Rockwood in view of Xie teaches this limitation. EX1002, ¶¶194-212,298-299.

- j. assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and**

Claim element 8[j] recites a limitation corresponding to the limitations recited in claim element 1[e]. As described above regarding claim 1[e], Rockwood discloses this limitation. EX1002, ¶¶214-226,298-299.

- k. transmit the assembled event line utilizing the communication interface.**

Claim element 8[k] recites a limitation corresponding to the limitations recited in claim element 1[f]. As described above regarding claim 1[f], Rockwood teaches this limitation. EX1002, ¶¶228-231,223-226. Further, Rockwood teaches transmitting the cited information relating to the event via the secure shell tunnel as described above regarding the claimed communication interface in limitation 8[c]. Thus, Rockwood discloses this limitation. EX1002, ¶¶298-299,304-306,310-312.

For the foregoing reasons, a PHOSITA would have found claim 8 of the '045 patent to be obvious in view of the combination of Rockwood and Xie. *Id.*, ¶¶298-313. Accordingly, claim 8 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

9. Claim 9

The system of claim 8, wherein the at least one of the one or more events is executed by the processor.

Rockwood teaches the events being transmissions on a network. Further, as explained above regarding claim 1[b], the network layer of the operating system

(OS) executes on a device and executes operations to transmit/receive packets via low-level network software of the OS. EX1004, 4:37-47,14:24-30; EX1002, ¶¶149-161,315. A PHOSITA would have understood that the manager server receives or transmits packets that constitute an event on the network such that the processor thereof executes the event. EX1002, ¶316.

Therefore, a PHOSITA as of the earliest possible priority date would have found the limitation recited in claim 9 to be obvious based on Rockwood. EX1002, ¶¶314-316. As shown, the Rockwood-Xie combination discloses all elements recited in claim 8 from which claim 9 depends. Accordingly, claim 9 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

10.Claim 10

The system of claim 8, further comprising:

a. a global perspective information server; and

Rockwood teaches a global server that receives detected events and operates with the global server and memory module of the system. EX1004, 4:39-47,5:10-25; EX1002, ¶¶320-323. Thus, Rockwood discloses this limitation.

- b. an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.**

As explained regarding claim limitation 1[e], Rockwood teaches a console having a GUI (corresponding to “end recipient device”) that displays information (e.g., as an “event line”) associated with a detected event and/or attacker profile (as modified by Xie) (corresponding to “originating object” in either mapping) including the source IP address associated with the transmitting network layer (corresponding to “first object” under the first mapping), the destination IP address, the attack timing, and packet payloads (corresponding to “first object” under the second mapping). EX1004, 7:39-60,8:6-67,9:59-61,10:39-41; EX1002, 194-212, ¶¶328. This information associated with the detected event and/or attacker profile can be stored on (and obtained from) the global server at least because the correlation is distributed on the global server and manager server. EX1004, 4:60-67; EX1002, ¶¶326-328.

Further, Rockwood discloses that the manager server together with the correlation engine (corresponding to “sensor agent”) transmits this information about the event (corresponding to “event line”) to the console. EX1004, 4:60-65,5:25-55; EX1002, ¶327. A PHOSITA would have understood the transmission of this information from the manager server (or interchangeably, the global server) to teach the limitation of “the information associated with the one or more of the

first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device” based on either of the first or second mappings used in claim 10. EX1002, ¶¶326-328.

Therefore, a PHOSITA would have found the limitations recited in claim 10 to be obvious based on Rockwood. EX1002, ¶¶319-329. As shown, the Rockwood-Xie combination discloses all elements recited in claim 8 from which claim 10 depends. Accordingly, claim 10 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

11. Claim 11

The system of claim 8, wherein the sensor agent is further operable to: cache the one or more events; and asynchronously consolidate and normalize the one or more events.

Rockwood discloses a correlation engine (corresponding to “sensor agent”) as part of the manager server or global server, where the correlation engine handles actions related to the events detected by sensors and stored by the memory module including retrieval and processing. EX1004, 5:1-15, Fig.-2; EX1002, ¶332.

Rockwood discloses that the correlation engine aggregates and stores event information that relates one event to other events on the network in the detected event storage of the memory module (corresponding to “cache the event and one or more other events”). EX1004, 6:63-67, 7:3-10; EX1002, ¶¶331-332.

Further, Rockwood teaches systems that receive events from sensors (at different times) into detected event storage which a PHOSITA would understand is asynchronous collection and consolidation. EX1002, ¶¶333-336; EX1004, 4:5-10. Further, the correlation engine operates to place the events in relation to other events based on attributes. EX1002, ¶¶333-336; EX1004, 6:35-48.

Therefore, a PHOSITA would have found the limitations recited in claim 11 to be obvious based on Rockwood. EX1002, ¶¶330-338. As shown, the Rockwood-Xie combination discloses all limitations of claim 8 from which claim 11 depends. Accordingly, claim 11 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

12. Claim 12

The system of claim 8, wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed.

Claim 12 recites limitations corresponding to the limitations recited in claim 4. EX1002, ¶¶339-340. As shown in the analysis of claim 4, Rockwood discloses the limitations recited in claim 12 under either mapping of “the first object.” EX1004, 4:45-60, 11:1-65; EX1002, ¶¶251-257, 339-340.

Therefore, a PHOSITA as of the earliest possible priority date would have found these limitations to be obvious based on Rockwood. *Id.* As shown, the Rockwood-Xie combination discloses all elements recited in claim 8 from which

claim 12 depends. Accordingly, claim 12 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

13. Claim 13

The system of claim 12, wherein the sensor agent is further operable to:

- a. determine whether the global perspective for the at least one event has been cached;**

Claim element 13[a] recites limitations corresponding to the limitations recited in claim 5[a]. As shown in the analysis of claim 5[a], Rockwood and Xie disclose the limitations recited in claim element 13[a]. EX1005, pp.29-38,64; EX1004, 5:1-15, 18:16-43; EX1002, ¶¶261-268,339-340. A PHOSITA would have been motivated to configure Rockwood-Xie's correlation engine ("sensor agent") such that it performs the steps of Claim 13. *Id.*, ¶¶341-342. Therefore, a PHOSITA would have found this limitation to be obvious in view of Rockwood and Xie. *Id.*

- b. when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and**

Claim element 13[b] recites limitations corresponding to the limitations recited in claim 5[b]. As shown in the analysis of claim 5[b], a PHOSITA would have understood that Rockwood-Xie disclose this limitation. EX1002, ¶¶270-271,339-340.

- c. when the global perspective for the at least one event has not been cached, obtain a global perspective for the at least one event from a community database.**

Claim element 13[c] recites limitations corresponding to the limitations recited in claim 5[c]. As shown in the analysis of claim 5[c], a PHOSITA would have understood that Rockwood-Xie disclose this limitation. EX1002, ¶¶274-278,339-40.

For the foregoing reasons, a PHOSITA as of the earliest possible priority date would have found the limitations recited in claim 13 to be obvious based on the Rockwood-Xie combination. EX1002, ¶¶339-344. As shown, the Rockwood-Xie combination discloses all elements recited in claims 8 and 12 from which claim 13 depends. Accordingly, claim 13 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

14.Claim 14

The system of claim 13, wherein the sensor agent is further operable to:

- a. determine whether the cached global perspective for the at least one event has expired; and**

Claim element 14[a] and the preamble recite limitations corresponding to the limitations recited in claim limitation 6[a]. As shown in the analysis of claim limitation 6[a], a PHOSITA would have understood that Rockwood-Xie discloses this limitation. EX1002, ¶¶282,339-340. A PHOSITA would have been motivated

to configure Rockwood-Xie's correlation engine ("sensor agent") such that it performs the steps of Claim 14. *Id.*

b. when the global perspective for the at least one event has expired, obtain a global perspective for the at least one event from a community database.

Claim element 14[b] recites limitations corresponding to the limitations recited in claim limitation 6[b]. As shown in the analysis of claim limitation 6[b], a PHOSITA would have understood that Rockwood-Xie discloses this limitation. EX1002, ¶¶282-289,339-340.

Therefore, a PHOSITA would have found the limitations recited in claim 14 to be obvious based on the Rockwood-Xie combination. *Id.* As shown, the Rockwood-Xie combination discloses all elements recited in claims 8, 12 and 13 from which claim 14 depends. Accordingly, claim 14 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

15. Claim 15

The system of claim 12, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

Claim 15 recites limitations corresponding to the limitations recited in claim 7. As shown in the analysis of claim 7, a PHOSITA would have understood that

Rockwood discloses the limitations recited in claim 15. EX1002, ¶¶290-297,339-340.

Therefore, a PHOSITA as of the earliest possible priority date would have found these limitations to be obvious based on Rockwood. EX1002, ¶¶339-344. As shown, the Rockwood-Xie combination discloses all elements recited in claims 8 and 12 from which claim 15 depends. Accordingly, claim 15 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

16. Claim 16

a. A system for providing forensic visibility into a system, comprising:

Rockwood discloses a manager server, a global server, and databases that host a n-dimensional graph of network events that provides an operator with a global view and visibility. EX1004, 4:5-17,14:24-34,20:50-60; EX1002, ¶345; limitation 8[a]. Accordingly, Rockwood discloses the preamble.

b. a device including:

Claim element 16[b] recites a limitation corresponding to the limitation recited in claim element 8[b]. EX1002, ¶345. As shown in the analysis of claim 8[b], Rockwood discloses this limitation. EX1002, ¶¶303-304,346.

c. a communication interface;

Claim element 16[c] recites a limitation corresponding to the limitation recited in claim element 8[c]. EX1002, ¶345. As shown in the analysis of claim 8[c], Rockwood discloses this limitation. *Id.*, ¶¶304-306,346.

d. a processor;

Claim element 16[d] recites a limitation corresponding to the limitation recited in claim element 8[d]. EX1002, ¶345. As shown in the analysis of claim 8[d], Rockwood discloses this limitation. *Id.*, ¶346.

e. data storage; and

Claim element 16[e] recites a limitation corresponding to the limitation recited in claim element 8[e]. EX1002, ¶345. As shown in the analysis of claim 8[e], Rockwood discloses this limitation. *Id.*, ¶346.

f. a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

Claim element 16[f] recites a limitation corresponding to the limitation recited in claim element 8[f]. EX1002, ¶345. As shown in the analysis of claim 8[f], Rockwood discloses this limitation. *Id.*, ¶346.

g. gather one or more events defining an action of a first object acting on a target;

Claim element 16[g] recites a limitation corresponding to the limitation recited in claim elements 8[g] and 1[b]. As shown in the analysis of claim elements 8[g] and 1[b], Rockwood discloses this limitation. EX1002, ¶¶143-161,298-299,345-346.

- h. generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;**

Claim element 16[h] recites a limitation corresponding to the limitation recited in claim elements 8[h] and 1[c]. As shown in the analysis of claim elements 8[h] and 1[c], Rockwood-Xie discloses this limitation. EX1002, ¶¶163-192,298-299,345-346.

- i. assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and**

As shown in the analysis of claim limitations 8[j] and 1[e], Rockwood-Xie discloses “assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object.” EX1002, ¶¶214-226,298-299,345-346. Disclosures of Rockwood-Xie that disclose limitation 1[d] (discussed for 1[d] above) also disclose “global perspective information comprising information about one or more related events to the one or more events across a network.” EX1002, ¶¶207-211,345-346.

j. transmit the assembled event line utilizing the communication interface.

Claim element 16[j] recites a limitation corresponding to the limitation recited in claim elements 8[k] and 1[f]. As shown in the analysis of claim elements 8[k] and 1[f], Rockwood-Xie discloses this limitation. EX1002, ¶¶228-231,345-347.

For the foregoing reasons, a PHOSITA as of the earliest possible priority date would have found claim 16 of the '045 patent to be obvious in view of the combination of Rockwood and Xie. EX1002, ¶¶345-348. Accordingly, claim 16 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

17. Claim 17

The system of claim 16, further comprising a global perspective information server including:

Rockwood teaches a global server that receives detected events and operates with the manager server and memory module of the system. EX1004, 4:39-47,5:10-25; EX1002, ¶¶351-358. Thus, Rockwood-Xie discloses this limitation.

a. a processor;

Rockwood teaches that the global server can be a computer or other processing device. EX1004, 4:39-47; EX1002, ¶¶351-357. Thus, Rockwood-Xie discloses this limitation. EX1002, ¶358.

b. a communication interface;

Rockwood teaches that the global server connects to the console and the system. EX1004, 4:39-47,5:15-37,14:25-27; EX1002, ¶¶360-362. Thus, Rockwood discloses this limitation. EX1002, ¶363.

c. data storage; and

Rockwood teaches that the memory module for the detected events may be disposed on the managing server and/or the global server. EX1004, 5:15-37; EX1002, ¶365. Thus, Rockwood discloses this limitation. EX1002, ¶366.

d. a global perspective module, wherein the global perspective module is operable to:

Rockwood teaches the global server includes an operating system and associated modules such as the correlation engine which a PHOSITA would have understood to teach the features of this limitation, or would have been motivated to configure the modules in such a manner. EX1004, 4:39-67; EX1002, ¶¶368-369. Thus, Rockwood discloses this limitation. *Id.*

e. receive the event line from the device;

Rockwood discloses that the global server operates at the highest logical level and connects to the manager servers to receive alerts and event information. EX1004, 2:40-65,4:7-67,5:60-65; EX1002, ¶¶372-373. Thus, Rockwood discloses this limitation. EX1002, ¶374.

- f. obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information;**

Claim element 17[f] recites a limitation corresponding to the limitations recited in claim element 1[d]. EX1002, ¶377. Further, the global server of Rockwood operates at the highest logical level and receives event information and related events (“global perspective”) from the manager server(s). EX1002, ¶¶377-379. As described above regarding claim 1[d], Rockwood or Rockwood in view of Xie teaches this limitation. EX1002, ¶¶194-212,376-380.

- g. assemble a second event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and**

Rockwood discloses that the global server collects detected event information including a number of attributes for each event. EX1004, 4:30-60; EX1002, ¶¶353,369,382. This event information is combined at both global server and manager server and is adjusted or focused at both servers into displayable representations of this information. EX1004, 2:45-65,7:1-25; EX1002, ¶¶353,369,382. Both Rockwood and Xie disclose aggregating information related to an event and compiling it for display (“assemble a second event line”). EX1005, pp.48,55; EX1004, 5:39-58; EX1002, ¶¶216-225,345-346,353,369,382. Further,

Rockwood discloses displaying information related to collected events and associated attributes, related events, and a target event in a graphical user interface (GUI) (corresponding to “a second event line including details associated with the at least one event”). EX1004, 7:5-37; EX1002, ¶¶216-225,345-346,353,369,382.

Further, Rockwood teaches the second part of the limitation, “the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object,” under either the first mapping or the second mapping as explained below.

In the first mapping of the network layer/OS of the source/transmitting device in Rockwood to the “first object,” Rockwood discloses that the information generated for display includes the packet payloads and headers for the event (corresponding to “information uniquely identifying...the action of the first object” (e.g., transmission of data)). EX1004, 5:39-58; EX1002, ¶¶216-225,345-346,353,369,382. The information generated in the system of Rockwood for display relative to the detected event also includes the attacker profile (as modified by Xie to include information on malware/source of an attack) (“information uniquely identifying...the originating object”). EX1004, 5:39-58,24:40-50; EX1002, ¶¶216-225,345-346,353,369,382. The network layer/OS (e.g., source IP, source port, and/or OS) (“information identifying each of the first object”) related to the event is collected and made viewable by the operator on a display as an

attribute of the event. EX1004, 12:19-67; EX1002, ¶216-225,345-346,353,369,382. Finally, the destination IP address of the event and packet (action) is also recorded and collected for display (“information uniquely identifying...the target”). EX1004, 7:5-10; EX1002, ¶216-225,345-346,353,369,382.

In the second mapping of the data package in Rockwood to the “first object,” Rockwood teaches that the information generated for display includes the packet payload (“information uniquely identifying each of the first object”), the attacker profile (as modified by Xie to include information on malware/source of an attack) (“information uniquely identifying...the originating object”), activity clusters (“information uniquely identifying...the action of the first object”), and the destination IP address (“information uniquely identifying...the target”), all related to an event or series of events (the information together teaches “second event line”). EX1004, 5:39-58,24:40-50; EX1002, ¶216-225,345-346,353,369,382. Thus, under either mapping, a PHOSITA would have understood that the system of Rockwood generates a second event line as recited in this limitation, the only differences being word choice. EX1004, 5:27-58,FIG.4,FIG.9; EX1002, ¶216-225,345-346,353,369,382.

Likewise, Xie discloses a similar aggregation of information in a multi-dimensional framework that is then displayed to visualize and trace the data

(corresponding to “second event line”) surrounding an event. EX1005, pp.42,48,55; EX1002, ¶216-225,345-346,353,369,382. Rockwood and Xie aggregate information in much the same way. EX1002, ¶216-225,345-346,353,369,382. Xie further discloses that the aggregated information is used to identify the particular type of malware (e.g., LION worm). EX1005, pp.46-49; EX1002, ¶216-225,345-346,353,369,382. Therefore, a PHOSITA would have looked to Xie to improve the system of Rockwood by providing additional capabilities for tracing events to malware (“information uniquely identifying...the originating object”) and the files containing the malware initiating the collected network actions. *Id.*

A PHOSITA would have recognized that Rockwood and Xie disclose aggregating event details described above which collectively disclose “the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object” as recited in this claim element. EX1002, ¶¶216-225,345-346,353,369,382. Thus, Rockwood and Xie disclose this limitation. *See also* discussion regarding limitation 1[e]. *Id.*, ¶383.

h. transmit the assembled second event line utilizing the communication interface to an end recipient.

As described above regarding claim limitations 1[f] and 8[k], Rockwood discloses this limitation. Specifically, the global server connects to the console

(corresponding to “end recipient”) via the communication interface described regarding claim element 17[b]. EX1002, ¶¶228-231,385-386.

Therefore, a PHOSITA as would have found claim 17 to be obvious in view of the combination of Rockwood and Xie. EX1002, ¶386. Accordingly, claim 17 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

18.Claim 18

The system of claim 17, wherein the end recipient heuristically displays information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object.

Claim element 18 recites limitations corresponding to the limitations recited in claim 7. As shown in the analysis of claim 7, a PHOSITA would have understood that Rockwood-Xie discloses this limitation. EX1002, ¶¶290-297,387-388. Further, the end recipient of this claim is taught according to the analysis provided regarding claim limitation 17[h]. EX1002, ¶¶387-388.

Therefore, a PHOSITA as of the earliest possible priority date would have found the limitations recited in claim 18 to be obvious based on Rockwood. *Id.*, 389. As shown, the Rockwood-Xie combination discloses all elements recited in

claim 17 from which claim 18 depends. Accordingly, claim 18 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

19. Claim 19

a. The system of claim 16, further comprising a bridge including:

Rockwood teaches a global server that receives detected events and operates with the manager server and memory module of the system in a manner that a PHOSITA would understand as a bridge. EX1004, 4:39-47,5:10-25; EX1002, ¶¶392-393. Thus, Rockwood-Xie discloses this limitation. *Id.*, 394.

b. a processor;

Rockwood teaches that the global server can be a computer or other processing device. EX1004, 4:39-47; EX1002, ¶¶392-393. Thus, Rockwood-Xie discloses this limitation. *Id.*, 394.

c. a communication interface;

Rockwood teaches that the global server connects to the console and the system. EX1004, 4:39-47,5:15-37,14:25-27; EX1002, ¶¶396-398. Thus, Rockwood discloses this limitation. *Id.*, 399.

d. a cached event store, wherein the cached event store is operable to:

Rockwood discloses that the global server could have an internal, external, or network-attached memory for storing events with a relevant program/module (“cached event store”). EX1004, 6:35-45; EX1002, ¶¶401-402. A PHOSITA would have understood that such a cached event store performed the steps of the

limitations below or would have been motivated to configure it in such a manner.

EX1004, 4:39-47; EX1002, ¶¶401-402. Thus, Rockwood discloses this limitation.

Id., 403.

e. receive a first request for a global perspective for the at least one event;

Rockwood discloses that the memory module, which includes detected event storage, can be remote from the global server and manager server. EX1004, 4:54-64,5:1-15; EX1002, ¶¶405-406. A PHOSITA would have understood that these servers would then make requests of the database at the memory module to retrieve the event attributes and event information for correlation and for the global view/perspective, or that a global server (together with its cached event store) can receive such requests from other devices/servers. EX1002, ¶¶405-406. Thus, Rockwood discloses this limitation. *Id.*, ¶407.

f. receive a second request for a global perspective for another event, the second request originating from another device;

Rockwood discloses that a global server is connected to multiple manager servers and the memory module (“cached event store”). EX1004, 4:5-47,5:61-63; EX1002, ¶409. Any one of these servers or the correlation engine distributed across the servers can access the memory module and retrieve detected events. EX1004, 4:5-47,5:60-67,15:10-19; EX1002, ¶409. Consoles (displays) connected

to the system also make multiple requests of the detected event storage. EX1004, 6:35-50,7:1-55.

Thus, Rockwood discloses this limitation. EX1002, ¶¶409-410. *See also* discussion regarding claim limitation 19[e].

- g. obtain a first global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information;**

Claim limitation 19[g] recites a limitation corresponding to limitations recited in claim elements 1[d] and 17[f]. EX1002, ¶413. Further, the global server (“bridge”) of Rockwood operates at the highest logical level and receives event information and related events (“first global perspective”) from the manager server(s). *Id.*, ¶¶412-415. As described above regarding claim 1[d], Rockwood or Rockwood in view of Xie teaches this limitation. *Id.*, ¶¶194-212,413-416.

- h. obtain a second global perspective for the another event;**

Rockwood discloses that various clusters of event information related to other event information (“second global perspective”) are queried from the correlation engine upon selection of a different event (“another event”). EX1004, 4:5-47,5:60-67,16:53-61; EX1002, ¶418. Thus, Rockwood-Xie discloses this limitation. EX1002, ¶¶418-419. *See also* discussion of limitation regarding 19[g].

i. provide the first global perspective to the device; and

Rockwood discloses that the system may include any number of consoles, each of which can connect to the memory module and the global server (cached event store) and manager servers. EX1004, 5:35-40,6:35-50; EX1002, ¶¶421-422. The cached event store delivers graphs (representing global perspective) based on any number of queries from the console. EX1004, 8:35-65. Thus, Rockwood-Xie discloses this limitation. EX1002, ¶¶421-423.

j. provide the second global perspective to the another device.

As described regarding claim limitation 19[i], Rockwood discloses that the system may include any number of consoles, each of which can connect to the memory module and the global server (cached event store) and manager servers. EX1004, 5:35-40,6:35-50; EX1002, ¶422,425. The cached event store delivers the graphs based on any number of queries from the console. EX1004, 8:35-65. EX1002, ¶425. Thus, Rockwood discloses this limitation. EX1002, ¶¶422,425-426.

For the foregoing reasons, a PHOSITA as of the earliest priority date would have found the limitations recited in claim 19 of the '045 patent to be obvious in view of the combination of Rockwood and Xie. EX1002, ¶¶392-426. As shown, the Rockwood-Xie combination discloses all elements recited in claim 16 from which claim 19 depends. Accordingly, claim 19 should be found invalid as unpatentable under 35 U.S.C. § 103 based on Rockwood in view of Xie.

VI. NO BASIS FOR DISCRETIONARY DENIAL

There is no basis to deny institution under 35 U.S.C. § 325(d).

There is parallel court litigation, so *Fintiv* factors are addressed preliminarily. First, no stay has been entered in the parallel litigation. Second, trial is currently set for August 19, 2024, so there is time to complete inter parte review. Third, it is early in the parallel litigation as fact discovery has not started. Fourth, Petitioner has identified the Rockwood and Xie prior art in Defendant's invalidity contentions filed in the parallel litigation. Finally, Petitioner and Webroot are parties in the parallel litigation as identified in the Mandatory Notices.

Discretionary denial is strongly disfavored here because the "same or substantially the same art or arguments" were not presented to the Office, and the Office "erred in a manner material" to patentability by not asserting the Rockwood and Xie references. See *Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6, 8-9 (Feb. 13, 2020). Analysis of this issue is guided by the "*Becton*" factors. *Id.* at 9-11.

Rockwood and Xie were not cited, individually or in combination, in any of the Office communications. See EX1006. Regarding *Becton* factors (a) (material differences between asserted art and prior art) and (b) (cumulative nature of the asserted art and prior art), Rockwood and Xie are materially different from the combination of references asserted in Office communications because Rockwood

and Xie disclose the independent claim limitations as discussed herein. Thus, the individual references of Rockwood and Xie are not merely cumulative of references the Office relied on. Regarding *Becton* factor (d) (extent of overlap), the arguments in this Petition do not overlap with arguments made during examination.

Even if the Board finds that the “same or substantially the same” art or arguments were presented to the Office, discretionary denial under § 325(d) is still not proper because the Office made a “material error” in not considering the Rockwood and Xie references.

Regarding *Becton* factors (c) (evaluation of art during examination), neither of Rockwood and Xie were used in any claim rejections, weighing strongly against exercising discretion. See *Cellco Partnership v. Huawei Device Co.*, IPR2020-01117, Paper 10, 13 (Feb. 3, 2021).

Regarding *Becton* factor (e) (examiner error) and (f) (other facts), this petition specifically points out and explains how Rockwood and Xie discloses all limitations of the claims.

VII. CONCLUSION

Inter partes review of claims 1-19 of U.S. Patent No. 9,578,045 is requested based on the grounds described above.

Respectfully submitted,

The Marbury Law Group, PLLC

A handwritten signature in black ink, reading "Robert M. Hansen", written over a horizontal line.

Robert M. Hansen, Reg. No. 43,656

Scott B. Amankwatia, Reg. No. 78,226

Matthew J. Anderson, Reg. No. 78,257

Attorneys for Petitioner

Date: March 6, 2023

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191
Tel: (703) 391-2900

CERTIFICATION OF SERVICE (37 C.F.R. §§ 42.6(e), 42.105(a))

The undersigned hereby certifies that the above-captioned **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 9,578,045**, Petitioner's power of attorney, and all associated exhibits were served in their entireties on March 6, 2023, on the following party via FedEx:

**Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
Austin TX 78705**


Robert M. Hansen, Reg. No. 43,656

Attorney for Petitioner

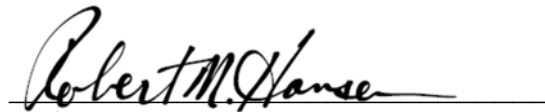
Date: March 6, 2023

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Tel: (703)-391-2900

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this Petition complies with the 14,000-word type-volume limitation. The Petition contains **13,846** words, excluding the table of contents, table of authorities, table of exhibits, mandatory disclosures, signature block, certificate of service, certificate of word count, and appendix of exhibits.

The Marbury Law Group, PLLC

A handwritten signature in black ink, reading "Robert M. Hansen", is written over a horizontal line.

Robert M. Hansen, Reg. 43,656
Attorney for Petitioner

Date: March 6, 2023

The Marbury Law Group, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, VA 20191

Tel: 703-391-2900