

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC, f/k/a, CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2023-00448
Patent No. 11,012,474

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE ’474 PATENT OVERVIEW	3
A. The ’474 Patent	3
B. Prosecution History	4
III. CLAIM CONSTRUCTION	5
IV. OVERVIEW OF THE CITED REFERENCES	7
A. Law	7
B. Golnabi	8
V. THE CHALLENGED CLAIMS ARE PATENTABLE	9
A. Ground 1: Claims 1-3, 5-7, 9-11, 13-15, 17-19, 21-23, 25-27, 29-31, and 33 Are Patentable Over Law in View of Golnabi.....	9
1. Patent at Claim 1; see also id. at Claims 9, 17. Substantially similar claim limitations are found in Independent Claim 25. For the reasons discussed as follows, Law taken alone or in combination with Golnabi does not disclose or render obvious the above-referenced limitations.....	10
2. Law does not teach or suggest the “rules automatically created or altered by an SPMS” limitation.	11
a. Law’s firm 305 does not disclose the claimed SPMS and its required functionality.	12
b. Law’s firm 305 does not disclose or render obvious the claimed SPMS and its required functionality.	14

3.	Law alone or in combination with Golnabi fails to teach or suggest the “rules added, removed, or altered” limitation.	17
a.	Dr. Jacobson’s hindsight-driven testimony retraces the inventors’ path.	18
b.	Petitioner fails to show that a POSITA would have been motivated to combine Law with Golnabi to arrive at the “rules, added, removed, or altered” limitation.....	21
4.	Law does not teach “an indication of a data feed” limitation	25
B.	Ground 2: Claims 2, 10, 18, and 26 are Patentable Over Law in View of Golnabi and Wood	27
C.	Ground 3: Claims 4, 12, 20, and 28 are Patentable Over Law in View of Golnabi and Ke.....	28
D.	Ground 4: Claims 5, 13, 21, and 29 are Patentable Over Law in View of Golnabi and Jungck.....	28
E.	Ground 5: Claims 7-8, 15-16, 23-24, and 31-32 are Patentable Over Law in View of Golnabi and Johnson.....	28
VI.	CONCLUSION.....	29

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>ADT LLC v. Vivint, Inc.</i> , No. IPR2022-00642, Paper 7 (P.T.A.B. Oct. 4, 2022)	26
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	16
<i>Google Inc. v. Koninklijke Philips N.V.</i> , No. IPR2017-00409, Paper 10 (P.T.A.B. June 5, 2017)	15
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	21
<i>In re Magnum Oil Tools Int'l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	15, 25
<i>Nichia Corp. v. Document Sec. Sys., Inc.</i> , No. 2020-2261, 2022 WL 1218036 (Fed. Cir. Apr. 26, 2022)	22
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	23, 24
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	5, 6
<i>Sprint Specturm L.P. v. Intellectual Ventures II LLC</i> , No. IPR2018-01765, Paper 11 (P.T.A.B. May 6, 2019)	23
<i>In re Stepan Co.</i> , 868 F.3d 1342 (Fed. Cir. 2017)	25
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	20
<i>Unigene Labs., Inc. v. Apotex, Inc.</i> , 655 F.3d 1352 (Fed. Cir. 2011)	20
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	26

<i>Xerox Corp. v. Bytemark, Inc.</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022).....	16, 18, 26
--	------------

Other Authorities

83 Fed. Reg. 51340, 51341 (Oct. 11, 2018).....	6
--	---

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Excerpts from The American Heritage Dictionary - "Firm" (4th ed. 2001)

I. INTRODUCTION

The Board should deny institution because Petitioner fails to show that Law (Ex. 1005) alone or in combination with Golnabi (Ex. 1009) or any of the other asserted references renders obvious the Challenged Claims.¹ Specifically, Petitioner fails to show that Law taken alone or in combination fails to disclose or render obvious several key limitations including, “rules automatically creates or altered by the security policy management server [SPMS],” rules added, removed or altered,” and “an indication of a feed” limitations.

First, Petitioner fails to show that Law teaches or suggests the “rules automatically created or altered by the SPMS” limitation. Petitioner relies on firm 305 (which it maps to the SPMS), however, firm 305 does not automatically update the operator-created rulesets. See Pet. at 28, 30-31. Firm 305, as a third-party company, still requires the use of IT personnel to update the rulesets specific to a process control system to ensure adequate protection. Law at ¶ 16 (disclosing that “IT personnel are still required to update the ruleset when new threats are discovered” to ensure that the updates provide the requisite protection), *id.* at ¶ 88

¹ Keysight Technologies, Inc., (“Petitioner”) petitioned for *inter partes* review of Claims 1-33 (the “Challenged Claims”) of U.S. Patent No. 11,012,474 (Ex. 1001, “the ’474 Patent”).

(disclosing that “a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc.”). Because IT personnel are a necessity in the updates, firm 305 does not provide automatic updates to rulesets.

Second, Law alone or in combination with Golnabi does not render obvious “rules added, removed, or altered . . . based on a correlation between portions of the malicious traffic information” (“an indication of a feed” limitation). Petitioner does not dispute that Law fails to disclose this limitation, as it must rely on its declarant, Dr. Jacobson’s, *ipse dixit* testimony and Golnabi to fill in the missing limitation. Dr. Jacobson’s conclusory testimony fails to show that a POSITA would have been guided by Law’s teachings to arrive at the limitation. Petitioner fails to explain how or why a POSITA would have combined Law with Golnabi to arrive at the limitation with a reasonable expectation of success.

Third, Law does not render obvious “an indication of a data feed.” Petitioner does not dispute that Law does not disclose this limitation and Petitioner’s only support for filling in the missing limitation comes once again from the conclusory *ipse dixit* testimony of Dr. Jacobson, which does not pass muster under *Xerox* and fails to show why firm 305 would have divulged the source of its paid-for feeds to Law’s process control system.

For at least these reasons, the Petition should be denied.

II. THE '474 PATENT OVERVIEW

A. The '474 Patent

The '474 Patent is directed to “[m]ethods and systems for protecting a secured network.” '474 Patent at Abstract, 1:57-8. Figure 1 shows a network environment having packet security gateways (“PSGs”) protecting networks A–D and an external security policy management server (“SPMS”) associated with the PSGs. *Id.* at 4:47-55, 5:19-29, FIG. 1.

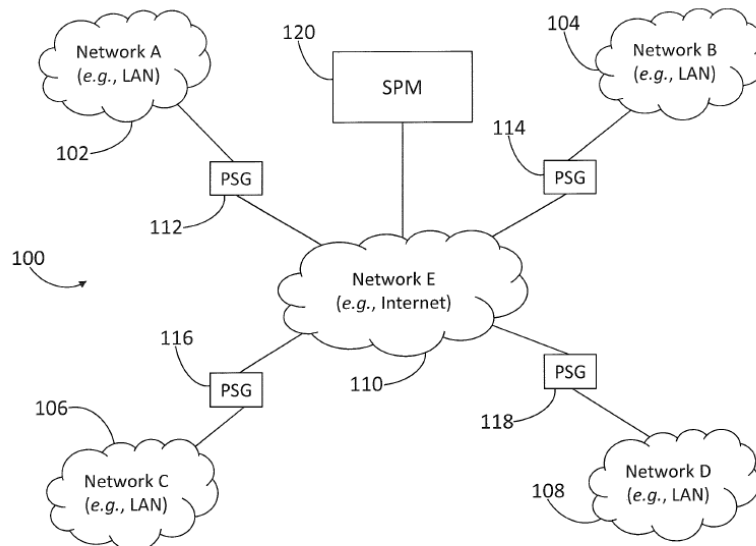


FIG. 1

Id., FIG. 1.

A PSG receives packets and proactively protects a network from malicious attacks based on dynamic security policies,² which include packet matching rules having packet matching criterion, packet transformation function, and an indication of a feed managed by a malicious host tracker server. *Id.* at 4:55-5:60, 11:52-66, 18:23-29, FIGS. 1, 5, 9, Claims 1, 9, 17, 25. The dynamic security policies are automatically created or altered by the SPMS based upon malicious traffic information received from several malicious host tracker services. *See id.* at 14:66-15:55.

As described and claimed in the '474 Patent, the SPMS receives security updates from multiple malicious host tracker services as part of a subscription. *See id.* at 15:30-55. The SPMS correlates the security updates and may combine, remove, or alter rules of dynamic security policies associated with the correlated updates. *See id.*

B. Prosecution History

During prosecution of the application that matured into the '474 Patent the Examiner rejected then-pending claims as being unpatentable over a combination of

² A dynamic security policy includes rules that “specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria.” '474 Patent at 7:30-33.

references. Ex. 1002 at 138-49. In response, Centripetal amended the claims by adding the following limitations:

- wherein at least two of the plurality of malicious host tracker services are managed by different organizations, wherein one or more of the packet filtering rules were added, removed or altered by the security policy management server based on a correlation between portions of the malicious traffic information; and
- wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services.

Id. at 63-72, 100-11.

Following the amendments, the Examiner issued a notice of allowance. *Id.* at 38-54. The Examiner determined that no art of record taken alone or in combination taught or suggested the amended claim language. *Id.* at 51-52.

III. CLAIM CONSTRUCTION

Under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005), patent claims are interpreted in light of the intrinsic evidence, including the specification and file history, and “the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application.”

Id. at 1313, 1317 (citation omitted); *see also* 83 Fed. Reg. 51340, 51341 (Oct. 11, 2018) (adopting *Phillips* standard for AIA proceedings before the Board).

Petitioner requests that the Board adopt constructions of the following claim terms that have been construed in previous IPR proceedings:

Term	The PTAB's construction
packet security gateway	a gateway computer configured to receive packets and perform a packet transformation function on the packets
packet transformation function	[one or more] operations performed on a packet
rule(s)	a condition or set of conditions that when satisfied causes a specific function to occur
dynamic security policy	any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria
security policy management server	a server configured to communicate a dynamic security policy to a packet gateway

See Pet. at 9-10. For the purpose of this Preliminary Response only, Centripetal adopts these constructions.

IV. OVERVIEW OF THE CITED REFERENCES

A. Law

While the '474 Patent leverages an SPMS to automatically create dynamic security policies and its packet filtering rules along with altering, adding or removing the rules based on correlating portions of malicious traffic information, Law does neither. See § II.A, *supra*; '474 Patent at Claims 1, 9, 17, 25.

In Law's disclosure, operators within the process control system environment (*e.g.*, a nuclear plant) create the "ruleset[s] [] specific to the system it protects." See Law at ¶ 16 (disclosing that "each ruleset is specific to the system it protects."), *id.* at ¶ 23 (disclosing that operating using a graphical process control system creates rulesets), *id.* at ¶ 90 (disclosing that the rulesets may be configured based on the operator or other personnel from a graphic display at a workstation in the process control system environment). By using the graphical displays, the operators create the rulesets (including a first set of rules) specific to a particular process control system.

Firm 305 is a third-party cyber security risk management company that provides a remediation service to update the operator-created rulesets. *Id.* ¶¶ 30, 88, 89. Unlike the claimed SPMS, which automatically creates or alters packet filtering rules, firm 305 is a company, such as Wurldtech Security, Inc., that employs IT personnel to update the operator-created rulesets when new threats are discovered.

See id. at ¶ 16 (disclosing that “IT personnel are still required to update the ruleset when new threats are discovered”), *id.* at ¶ 88 (“With reference to FIG. 3, a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc. of Vancouver, BC Canada” provides the updates). Because “each ruleset is specific to the system it protects,” IT personnel “are still required to update the ruleset when new threats are discovered” to ensure that the update provides the required protection. *Id.* at ¶ 16. Thus, firm 305 necessitates manual updates to the rulesets protecting a process control system.

Additionally, firm 305 does not alter, add, or remove rules, let alone based on correlating threat data, when updating the operator-created rulesets. While the operator-created rulesets are updated based on threat data 310, Law does not disclose duplicate rules or remove any such rules based on any correlation of the threat data. *See* Law at ¶ 88, Fig. 3.

B. Golnabi

Golnabi is cited for its disclosure of generating policy rules for firewalls. Golnabi generates policy rules based on its aggregation technique, which combines a group of similar rules (*e.g.*, based on attributes) into a “superset of all rules identified,” (Golnabi at 312) as illustrated in Figure 7:

```
► 1 TCP,INPUT,129.110.96.117,ANY,129.110.96.80,22,DENY
  2 TCP,INPUT,129.110.96.117,ANY,129.110.96.80,80,DENY
  3 UDP,INPUT,*,*,*,ANY,10.110.96.255,ANY,DENY
  4 UDP,OUTPUT,129.110.96.80,ANY,129.110.10.*,ANY,DENY
  5 TCP,INPUT,*,*,*,ANY,129.110.96.80,80,ACCEPT
  6 UDP,INPUT,129.110.10.*,53,129.110.96.80,ANY,ACCEPT
  7 UDP,OUTPUT,129.110.96.80,ANY,129.110.96.*,53,ACCEPT
```

Figure 7. Generalized Filtering Rules

Id. at Fig. 7; *see also id.* at 308-10. To achieve this grouping, Golnabi mines the attribute data from firewall log data. *See id.* at 307-08 (disclosing that the process consists of extracting from the firewall log data attributes for data mining), *id.* at 312 (disclosing that the firewall log data includes packet information, including source and destination IP addresses).

V. THE CHALLENGED CLAIMS ARE PATENTABLE

A. Ground 1: Claims 1-3, 5-7, 9-11, 13-15, 17-19, 21-23, 25-27, 29-31, and 33 Are Patentable Over Law in View of Golnabi

Independent Claims 1, 9, 17, and 25 require, *inter alia*, that:

- “wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services” (“rules automatically created or altered by the SPMS” limitation);
- “wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information” (“rules added, removed, or altered” limitation); and

- “a first packet matching rule of the packet filtering rules comprises . . . an indication of a feed managed by at least one of the plurality of malicious host tracker services” (“an indication of a feed” limitation).

1. Patent at Claim 1; see also id. at Claims 9, 17. Substantially similar claim limitations are found in Independent Claim 25. For the reasons discussed as follows, Law taken alone or in combination with Golnabi does not disclose or render obvious the above-referenced limitations.

First, Law does not disclose an SPMS that automatically creates or alters rules. Petitioner maps firm 305 to the claimed SPMS and functionality, but firm 305, as a third-party company, still requires the use of IT-personnel to update rulesets when new threats are required to ensure that the updates provide the required protection for the process control system. Law at ¶¶ 16, 88. Accordingly, firm 305 does not automatically update rulesets.

Second, Law alone or in combination with Golnabi does not alter, add, or remove packet filtering rules of a dynamic security policy based on correlating malicious traffic information. Petitioner does not dispute that Law fails to disclose removing duplicate rules based on correlating threat data. See Pet. at 37. As such, Petitioner resorts to Dr. Jacobson's hindsight-driven and conclusory testimony, and in the alternative, Golnabi for the missing limitation, without any explanation for how or why a POSITA would have been motivated to make the combination and

have a reasonable expectation of success in arriving at the “rules added, removed, or altered” limitation. *See id.* at 37-38.

Third, Law does not teach or suggest packet filtering rules including an indication feed. Petitioner does not dispute that Law fails to disclose this limitation and once again relies on Dr. Jacobson's conclusory testimony to supply the missing limitation. *See id.* at 42. Focusing only on the process control system, the conclusory testimony fails to explain why firm 305 itself would have divulged the source of its threat data to allow an operator of Law's process control system to access rulesets with an indication feed.

2. Law does not teach or suggest the “rules automatically created or altered by an SPMS” limitation.

Under the construction adopted by the Board in previous IPRs, the claimed SPMS means “a server configured to communicate a dynamic security policy to a packet gateway.” *See* § IV, *supra*. In addition to this requirement, the Challenged Claims also require that the claimed SPMS automatically creates or alters a first set of packet filtering rules. *See* '474 Patent at Claim 1 (“one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered”); *see also id.* at Claims 9, 17, and 25. Petitioner fails to show that Law's firm 305 discloses or renders obvious the claimed SPMS and required functionality of automatically creating or altering the rules.

a. Law's firm 305 does not disclose the claimed SPMS and its required functionality.

Petitioner alleges that firm 305 is itself a server that automatically constructs and distributes ruleset 147. *See* Pet. at 28, 31-32. But Law defines firm 305 as a commercial company, such as Wurldtech Security, Inc. Law at ¶ 88 (“a third party, cyber security risk management firm 305 such as Wurldtech Security, Inc.”); *see also* Ex. 2001 at 3 (defining “firm” as meaning “[a] commercial partnership of two or more persons.”).

More specifically, Law explains that firm 305 is a “third party, cyber security risk management firm [] such as Wurldtech security, Inc.” that, as a company, provides a remediation update service to the process control system. Law at ¶ 88, *id.* at ¶ 89 (indicating that “firm 305 may provide an ongoing remediation update service to the system 100 in the form of UTMS-device updates” to rules in ruleset 147); *see also id.* at ¶¶ 22, 30. To provide this remediation update service, firm 305 necessarily employs IT personnel and uses multiple components to update rulesets specific to the process control system they protect. *See, e.g., id.* at ¶ 16 (explaining that because process control systems are unique, third-party management still requires “IT personnel . . . to update the ruleset when new threats are discovered.”). Thus, firm 305 (external to the process control system) requires the involvement of IT personnel to ensure that updated rulesets provide the requisite protection. *Id.*

Petitioner's citation to paragraph 83 does not show otherwise. *See* Pet. at 28, 31. Petitioner cites paragraph 83's passage of "automatic updates of the ruleset 147" to allege that firm 305 automatically updates rulesets. *Id.* (quoting Law at ¶ 83) (quotations omitted). It does not. By reading Law's passage in isolation, Petitioner mistakenly conflates the process control system that performs automatic updates with that of external firm 305. *Id.* Specifically, paragraph 83 is directed to the process control system, not firm 305:

Generally speaking, a set of predefined graphic elements may be provided in the configuration application to enable a user to construct ***process graphic displays that reflect the process plant and the process control system 100*** in general and include visual representations of the UTMS-configured firewall devices as described above Detection of certain network conditions may also trigger an automatic update of the rulesets 147, 148, 151, 153 or an alarm to prompt a user to perform a manual update of the rulesets or another action to fully secure the system 100.

Law at ¶ 83 (emphasis added); *see also id.* at ¶¶ 81, 82 (describing access to the user interfaces located within the process control system to allow for ruleset configuration, updates, and accepting ruleset updates).

As Law discloses that within the process control system, predefined graphic elements are provided "to enable a user to construct process graphic displays that reflect the process plant and process control system." *Id.* at ¶ 83; *see also id.* at Fig.

2 (showing user-defined profiles 232). In this way, graphic displays allow operators within the process control system to either “perform a manual update of the rulesets” or set “an automatic update” upon “[d]etection of certain network conditions.” *Id.* at ¶ 83. Accordingly, while the process control system manages updates to ruleset 147 either manually or automatically, there is no disclosure or contemplation that external firm 305 automatically updates ruleset 147. Nor could there be. Because, as explained above, IT personnel outside the system are still required to update rulesets when new threats are detected. *Id.* at ¶ 16.

Petitioner, therefore, makes an insufficient showing that Law discloses that firm 305 performs automatic updates to ruleset 147 to satisfy the claimed SPMS that automatically creates or alters rules in ruleset 147.

b. Law's firm 305 does not disclose or render obvious the claimed SPMS and its required functionality.

Petitioner also argues in the alternative that Law renders obvious automatically creating or altering rules by firm 305. *See* Pet. at 30-31. Petitioner's obviousness argument lacks substantiated evidence in view of Law's disclosure which shows involvement by third-party IT personnel.

As established above, Law explains that process control systems greatly differ from that of typical IT environments and require uniquely trained third-party IT personnel to update operator-created rulesets specific to the process control systems they protect. *See* § V.A, *supra*. Therefore, in constructing updates to rulesets, IT

personnel of firm 305 are instrumental in the updates when new threats are discovered to ensure that the updated rulesets provide the necessary protection. Law at ¶ 88; *see also* ¶ 16 (“IT personnel are still required to update the ruleset when new threats are discovered” and must understand how and why the rulesets need to be changed to protect the specific process control system). Accordingly, third-party IT personnel may construct the updated rulesets and run tests to ensure that the “rulesets effectively secure the process control systems in a desirable manner,” all of which can be performed offline, *i.e.* not on a server. *Id.* at ¶ 88. In this manner, IT personnel and offline computing components are necessarily involved in the updating process.

Critically, Petitioner ignores these unique and necessary third-party IT personnel requirements in referencing alleged “known techniques for automatically generating rules” and asserting “[i]t would have been obvious to a POSITA to incorporate [in firm 305].” Pet. at 30. Petitioner’s assertion is conclusory and lacks evidentiary support from Law itself. *See In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (a petitioner’s burden of proving obviousness cannot be satisfied by employing “mere conclusory statements”); *see also Google Inc. v. Koninklijke Philips N.V.*, No. IPR2017-00409, Paper 10 at 13-14 (P.T.A.B. June 5, 2017) (denying institution based in part on petitioner’s conclusory statements that lacked reasoned analysis and evidentiary support.). In fact, Petitioner’s only

support for this assertion is from Dr. Jacobson who merely repeats, verbatim the assertion for which it is offered for support. *See* Ex. 1003, ¶ 71; *see Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15-16 (P.T.A.B. Aug. 24, 2022) (precedential).

Equally problematic is that Petitioner dispensed with “provid[ing] adequately developed explanations” when relying on the alleged techniques for automatically generating rules. *See* Pet. at 30; *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015) (case law has “not dispense[d] with the need for parties to provide adequately developed explanations when relying on background knowledge based on cited art.”) (citation omitted). Other than saying that automatic generation was allegedly known, Petitioner does not provide an adequate explanation for why a POSITA would have incorporated such an alleged technique in firm 305 or how such incorporation would have ensured that each ruleset update is specific to the particular process control system and its particular security needs without the involvement of IT personnel that are “still required to update rulesets when new threats are discovered.” Law at ¶¶ 16, 88. Law’s firm 305 is not one that automatically updates rulesets, but instead, one that relies on the expertise and knowledge of the firm’s IT personnel to construct rules based on their understanding of the network topography of Law’s process control system and the particular needs of the devices it contains. *See id.*

3. Law alone or in combination with Golnabi fails to teach or suggest the “rules added, removed, or altered” limitation.

The '474 Patent specification provides that the SPMS may add, remove, or alter, dynamic security policies stored in the SPMS memory. '474 Patent at 15:30-32 (disclosing that the “security policy management server 120 may be configured to add, remove, and/or alter one or more dynamic security policies stored in memory.”). To update the stored dynamic security policies, the specification describes that the SPMS correlates information, *e.g.*, network addresses, from two or more services and, for example, “combine[s] the rules associated with the[] correlated updates from two or more services within one or more dynamic security policies.” *Id.* at 15:44:47. Consistent with this description, the Challenged Claims recite “one or more of the packet filtering rules [that] were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information.” *See* '474 Patent at Claims 1, 9, 17, 25.

Petitioner concedes that Law does not disclose the “rules added, removed, or altered” limitation. *See* Pet. at 37. As such, Petitioner resorts to Dr. Jacobson's *ipse dixit* testimony to supply the missing limitation and, if that is not enough, turns to Golnabi. *Id.* at 37-38 (citing Dr. Jacobson's declaration (Ex. 1003) and then turning to Golnabi). However, neither Dr. Jacobson's testimony nor Golnabi is sufficient to

show that Law, alone or taken in combination with Golnabi, does not teach or suggest the “rules, added, removed, or altered” limitation.

a. Dr. Jacobson's hindsight-driven testimony retraces the inventors' path.

Petitioner's only record support for the assertion that Law taken alone renders obvious the “rules, added, removed, or altered” limitation is Dr. Jacobson's testimony. *See* Pet. at 37 (citing Ex. 1003 at ¶ 79). However, Dr. Jacobson “offers only a verbatim restatement of the assertion being supported, without any supporting evidence or technical reasoning,” which under the precedential decision in *Xerox* is entitled to little to no weight. Paper 9 at 15-16 (denying institution where expert testimony merely repeats, verbatim the conclusory assertion for which it is offered to support.). Dr. Jacobson asserts in a conclusory fashion that “it would have been obvious to a POSITA to analyze the received threat data 310 to remove duplicate rules.” Ex. 1003 at ¶ 79 (relying on ruleset 147 for the modifications). To make this assertion, Dr. Jacobson reads Law through the lens of hindsight because Law does not teach or otherwise contemplate such a process.

Firm 305 simply updates rules in ruleset 147 based on aggregated threat data 310 with no contemplation of removing duplicate rules. Law at ¶ 88, Fig. 3. Petitioner does not dispute this. Pet. at 37. To accomplish this update, firm 305 simply collects threat data 310 and then uses the collected threat data 310 to construct the updated rules in ruleset 147. *See id.* at ¶ 88 (In reference to the method

of updating rulesets as in figure 3, firm 305 “**collect[s]** the threat data 310 from the World Wide Web using various data collection techniques (e.g., robots, crawling, data feeds, collaborative forums, etc.), **construct[s]** data files to convey the rulesets to their destination devices in a device-compatible manner”) (emphasis added). There is no teaching or suggestion of removing any duplicate rules, much less based on correlating threat data.

Dr. Jacobson's conclusory testimony that it would have been obvious to analyze threat data to “remove duplicate rules [in ruleset 147]” is wrong. Ex. 1003 at ¶ 79 (relying on ruleset 147 in the proposed analysis of threat data). Dr. Jacobson rests his testimony on the removal of duplicate rules in ruleset 147 based on the analysis of threat data, but because the ruleset was created by the operator in the process control system, there are no duplicate rules. See Law at ¶¶ 21, 23, 81, 90 (“the rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120.”). At best, the threat data would be analyzed to remove any duplicative information in the data rather than the operator-created ruleset in order to avoid constructing unnecessary duplicate rules. Accordingly, there is no removal of duplicate rules created based on threat data from different sources that are removed after construction based on analyzing the threat data.

To put a finer point on it, a POSITA would have found it more efficient to analyze the received threat data and “remove” any duplicate information **before** constructing updates to ruleset 147, as opposed to constructing (potentially numerous) duplicate rules, comparing the received threat data and then removing the constructed duplicate rules in the updated ruleset 147. *See id.* at ¶ 88 (collect threat data and then construct updates to rulesets). Accordingly, Law does not guide a POSITA to correlate threat data to remove duplicate rules in ruleset 147, but to remove duplicate threat data **before** constructing updates to ruleset 147 instead. *See Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1361 (Fed. Cir. 2011) (“To render a claim obvious, prior art cannot be ‘vague’ and must collectively, although not explicitly, guide an artisan of ordinary skill towards a particular solution.”) (citation omitted).

Because the prior art did not guide the combination, it is axiomatic that Dr. Jacobson used the '474 Patent itself as a roadmap to construct the Petition's obviousness theory. *See* Ex. 1003 at ¶¶ 78-79; *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1357-62 (Fed. Cir. 2019). In fact, Dr. Jacobson cites the '474 Patent for explaining how the correlation would work “to find the duplicates, and the ruleset altered by removing the duplicates” for efficiency. Ex. 1003 at ¶ 78 (citing '474 Patent 15:7-55); Pet. at 37. The '474 Patent accordingly guided Dr. Jacobson's to conclude that “it would have been obvious to a POSITA to analyze the received

threat data 310 to remove duplicate rules.” Ex. 1003 at ¶ 79. Thus, Dr. Jacobson “read into the prior art the teachings of the invention in issue,” which is hindsight. *Graham v. John Deere Co.*, 383 U.S. 1, 36 (1966).

b. Petitioner fails to show that a POSITA would have been motivated to combine Law with Golnabi to arrive at the “rules, added, removed, or altered” limitation.

Recognizing that its single reference obvious theory lacks merit, Petitioner resorts to a combination of Law with Golnabi’s aggregation technique. See Pet. at 37-38 (alleging that “[i]t would have been obvious to a POSITA to combine rules as Golnabi teaches [an aggregation technique] when constructing rulesets.”). This combination is also deficient for at least several reasons.

First, as established above, a POSITA would not have found it obvious to construct (potentially numerous) rules in updating ruleset 147 and then correlate the threat data to remove the duplicated rules. Petitioner does not rectify this fatal deficiency when alleging that it would have been obvious to use Golnabi’s aggregation technique in constructing updates to Law’s rulesets. See *id.* at 38.

Second, Petitioner fails to provide any meaningful explanation for how or why a POSITA would have incorporated Golnabi’s technique into Law to arrive at the “rules, added, removed, or altered” limitation. See Pet. at 38; *id.* at 18-19. For example, Petitioner fails to explain why a POSITA would have looked to Golnabi’s technique for the removal of duplicate rules in ruleset 147. Golnabi’s central

objective is to generate new firewall policy rules based on an aggregation technique that combines a group of overlapping ranges of IP addresses. See Golnabi at Abstract (describing its goal “to generate a new set of efficient firewall policy rules”), *id.* at 308 (describing its goal to “generate a minimum number of firewall policy rules”), *id.* (achieving the goal based on the “aggregat[ion] for its corresponding range of IP addresses or port numbers or even to be “ANY” or “*” to cover all the specified range, for the corresponding firewall rules.”), *id.* at 309 (disclosing that “[f]or example the IP addresses of 129.110.10.7 and 129.110.10.1 can be aggregated to 129.110.10.*”). Petitioner’s proposed combination, on the other hand, rests upon the removal of duplicate rules in Law. See Pet. at 37-38.

Petitioner fails to reconcile Golnabi’s objective of generating new rulesets based on aggregation with its proposed approach of “remov[ing] duplicate rules” in its Law-Golnabi combination. Compare Golnabi at Abstract (Golnabi’s technique is “to generate a new set of efficient firewall policy rules.”) with Pet. at 38 (“processing the received threat data to remove duplicate rules would have been obvious over Law in view of Golnabi”); see also *id.* at 37. In fact, Petitioner does not even try as it shifts its theory from the “remov[al] of duplicate rules” to that of combining rules in the very last sentence of the Law-Golnabi analysis. See Pet. at 38; *Nichia Corp. v. Document Sec. Sys., Inc.*, No. 2020-2261, 2022 WL 1218036, at

*4 (Fed. Cir. Apr. 26, 2022) (the challenger “must provide an understandable explanation of the element-by-element specifics of its unpatentability contentions”).

Petitioner does not appear to appreciate this (or any) distinction between removal of duplicate rules and the aggregating overlapping rules as the '474 Patent points out. See '474 Patent at 15:52-55 (“For example, duplicate network addresses may be removed, *and/or* overlapping ranges of network addresses may be combined into one or more new network address ranges.”) (emphasis added); see also Golnabi at 309 (“For example, the IP addresses of 129.110.10.7 and 129.110.10.1 can be aggregated to 129.110.10.*” when dealing with overlapping network addresses). Petitioner, therefore, fails to provide any understandable explanation as to why a POSITA would have looked to Golnabi's aggregation technique for Law.

Third, even assuming *arguendo* that a POSITA would have looked to Golnabi's aggregated technique for Law, Petitioner fails to show how Golnabi's aggregated technique would be implemented in Law to serve the purpose of the proposed combination. See *Sprint Spectrum L.P. v. Intellectual Ventures II LLC*, No. IPR2018-01765, Paper 11 at 25 (P.T.A.B. May 6, 2019) (denying institution because the petitioner failed to demonstrate how a reference's algorithms would be modified to serve the purpose of the proposed combination) (citing *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017)). That is, Petitioner fails to explain how Golnabi's aggregation technique would or even could be

modified in Law to serve the purpose of removing altogether duplicate rules based on *correlating portions of malicious traffic information*, as required by the Challenged Claims.

To generate new rulesets, Golnabi's aggregation technique factors in attributes of a packet (*e.g.*, IP address or port number fields) based on mining firewall log files. Golnabi at 307 (explaining the overall process of mining log file), *id.* at 307-08 (explaining the process of extracting the attributes of a packet from the log). Given that Golnabi's aggregation technique is based on mining firewall log files, Petitioner fails to provide the required explanation for how the combination as proposed would be expected to work in using threat data from third party sources instead of mined firewall log file attributes as in Golnabi. *See Pers. Web Techs.*, 848 F.3d at 994 (vacating and remanding the Board's obviousness findings because the "Board nowhere clearly explained, or cited evidence showing, *how* the combination of the two references was supposed to work.").

Fourth, and dovetailing with the foregoing, Petitioner does not even address whether a POSITA would have had a reasonable expectation of success for the proposed modification of Golnabi's technique in Law. *See Pet.* at 18-19. A party that petitions the Board for a determination of unpatentability based on obviousness must show that "a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the

skilled artisan **would have had a reasonable expectation of success in doing so.**” *In re Magnum Oil Tools*, 829 F.3d at 1381 (emphasis added) (citations omitted); see *In re Stepan Co.*, 868 F.3d 1342, 1346 n.1 (Fed. Cir. 2017) (“there must be a motivation to make the combination and a reasonable expectation that such a combination would be successful, otherwise a skilled artisan would not arrive at the claimed combination.”). Petitioner’s lack of support for any reasonable expectation of success is another reason for why Petitioner fails to show that a POSITA would have been motivated to combine Law with Golnabi and have a reasonable expectation of success to arrive at the claimed invention.

4. Law does not teach “an indication of a data feed” limitation

Law does not satisfy “an indication of a feed” limitation under the plain reading of the claim. The plain language of “an indication of a feed” requires an identification of a feed. ’474 Patent at Claims 1, 9, 17, and 25 (“***an indication of a feed*** managed by at least one of the plurality of malicious host tracker services”) (emphasis added). Petitioner acknowledges this explicit requirement. See Pet. at 42 (“an identification of a feed” refers to “identifying the feed”).

Petitioner concedes that Law does not disclose identifying a feed, *e.g.*, information regarding source 315. *Id.* As such, Petitioner resorts to an obviousness theory instead, asserting that:

[I]t would have been obvious to a POSITA that information regarding the source 315 of each rule may be helpful to a user when using the ruleset interface to configure and control any of the rules within rulesets [T]herefore it would have been obvious to communicate that information to a user.

Id. at 42-43 (citing Ex. 1003 at ¶ 87). As an initial matter, the only support for this assertion is Dr. Jacobson's testimony, which again, is a verbatim restatement of the assertion for which it is offered to support. *See Xerox*, Paper 9 at 15-16.

Moreover, merely stating that "information regarding the source of each 315 may be helpful to a user" is akin to concluding that "it would have been obvious." *See In re Van Os*, 844 F.3d 1359, 1361-62 (Fed. Cir. 2017) (explaining that "a finding that a combination of prior art would have been . . . 'intuitive' is no different than merely stating the combination 'would have been obvious'"); *see also ADT LLC v. Vivint, Inc.*, No. IPR2022-00642, Paper 7 at 17 (P.T.A.B. Oct. 4, 2022) (denying institution based, in part, on petitioner's statement of "better monitoring and management of personnel, asset and field devices" is "akin to stating in a conclusory fashion that the proposed combination 'would have been obvious.'" (citing *In re Van Os*, 844 F.3d at 1362).

Petitioner's conclusory assertion that "it would have been obvious to communicate that information to a user [of the process control system]" (Pet. at 43) fails to provide any factual or evidentiary underpinnings as to ***why firm 305 would***

have had reason to divulge the source of its paid-for “research subscription feeds” to the process control system. Ex. 1007 at 5 (“Assurent’s principal Vulnerability Research Offerings include: Vulnerability Research Subscription feeds”); Law at ¶ 92 (Law’s firm 305 collects threat data from Assurent Secure Technologies). Accordingly, while this information regarding the source may be helpful to an operator in the process control system, Petitioner provides no articulated reasoning as to how or why a POSITA could have even obtained from firm 305 its proprietary and paid-for subscription feeds to modify Law’s rulesets with an indication feed.

In view of the foregoing, Petitioner fails to show that Law teaches or suggest “an indication of a feed” limitation.

* * *

For at least the foregoing reasons, Petitioner certainly cannot satisfy its burden to move forward to trial.

B. Ground 2: Claims 2, 10, 18, and 26 are Patentable Over Law in View of Golnabi and Wood

Petitioner has not demonstrated a reasonable likelihood that Independent Claims 1, 9, 17, and 25 are obvious over Law in view of Golnabi, and Wood (Ex. 1006) does not cure any of the above-noted deficiencies. See § VI.A, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 2, 10, 18, and 26, which depend from the independent claims, are unpatentable over Law in view of Wood.

C. Ground 3: Claims 4, 12, 20, and 28 are Patentable Over Law in View of Golnabi and Ke

Petitioner has not demonstrated a reasonable likelihood that Independent Claims 1, 9, 17, and 25 are obvious over Law in view of Golnabi, and Ke (Ex. 1010) does not cure any of the above-noted deficiencies. *See* § VI.A, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 4, 12, 20, and 28, which depend from the independent claims, are unpatentable over Law in view of Golnabi and Ke.

D. Ground 4: Claims 5, 13, 21, and 29 are Patentable Over Law in View of Golnabi and Jungck

Petitioner has not demonstrated a reasonable likelihood that Independent Claims 1, 9, 17, and 25 are obvious over Law in view of Golnabi, and Jungck (Ex. 1008) does not cure any of the above-noted deficiencies. *See* § VI.A, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 5, 13, 21, and 29, which depend from the independent claims, are unpatentable over Law in view of Golnabi and Jungck.

E. Ground 5: Claims 7-8, 15-16, 23-24, and 31-32 are Patentable Over Law in View of Golnabi and Johnson

Petitioner has not demonstrated a reasonable likelihood that Independent Claims 1, 9, 17, and 25 are obvious over Law in view of Golnabi, and Johnson (Ex. 1011) does not cure any of the above-noted deficiencies. *See* § VI.A, *supra*. Accordingly, Petitioner fails to demonstrate a reasonable likelihood that Claims 7-

8, 15-16, 23-24, and 31-32, which depend from the independent claims, are unpatentable over Law in view of Golnabi and Johnson.

VI. CONCLUSION

For the foregoing reasons, institution should be denied.

Respectfully submitted,

Dated: May 9, 2023

By: /James Hannah /
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800
Email: jhannah@kramerlevin.com
Email: jfuller@kramerlevin.com

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302
Email: jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Email: skelly@bannerwitcoff.com
Email: bwright@bannerwitcoff.com
Email: jhutchins@bannerwitcoff.com

Attorneys for Patent Owner

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the portions of the foregoing PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. § 42.24 has 6,370 words in compliance with the 14,000-word limit set forth in C.F.R. § 42.24(b)(1). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: May 9, 2023

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
Kramer Levin Naftalis & Frankel LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: (650) 752-1700 Fax: (650) 752-1800
Email: jhannah@kramerlevin.com
Email: jfuller@kramerlevin.com

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: (212) 715-7502 Fax: (212) 715-8302
Email: jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John R. Hutchins (Reg. No. 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Email: skelly@bannerwitcoff.com
Email: bwright@bannerwitcoff.com
Email: jhutchins@bannerwitcoff.com

Attorneys for Patent Owner

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, that service was made on Petitioner as detailed below.

<i>Date of service</i>	May 9, 2023
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S PRELIMINARY RESPONSE
<i>Persons served</i>	Gerard M. Donovan Peter J. Chassman Jonathan I. Detrixhe Sidharth Kapoor REED SMITH LLP gdonovan@reedsmith.com pchassman@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Lead Counsel for Patent Owner