

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

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

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
I. THE '474 PATENT OVERVIEW	3
II. LEVEL OF ORDINARY SKILL IN THE ART	6
III. CLAIM CONSTRUCTION	7
IV. OVERVIEW OF THE REFERENCES	8
A. The Law Reference	8
B. The Golnabi Reference	10
V. THE CHALLENGED CLAIMS ARE PATENTABLE	11
A. Law Does Not Disclose Nor Render Obvious a Security Policy Management Server That Automatically Creates or Alters Dynamic Security Policies	11
1. Law Does Not Disclose the Automatic Generation of Rulesets by Firm 305	12
2. Skilled Artisans Would Not Have Found it Obvious to Incorporate Automatic Generation Techniques in Firm 305 Because IT Personnel Are Required For the Updates	15
B. Law in View of Golnabi Does Not Disclose Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlating Malicious Traffic Information	19
1. Law Does Not Disclose This Limitation, and the Alleged Motivation to Modify Law is the Product of Hindsight	20
2. Petitioner's Alternative Theory of Law in View of Golnabi Also Does Not Reach the Claimed Invention	25

C. Law Does Not Disclose Nor Render Obvious a PSG Receiving
From an SPMS a Dynamic Security Policy With Rules
Including Indications of Feeds Managed by Malicious Host
Tracker Services 28

VI. CONCLUSION.....34

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Arendi S.A.R.L. v. Apple Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	31
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	16
<i>Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc.</i> , 796 F.2d 443 (Fed. Cir. 1986)	27
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	26
<i>Chemours Co. FC, LLC v. Daikin Indus., Ltd.</i> , 4 F.4th 1370 (Fed. Cir. 2021)	16
<i>Interconnect Planning Corp. v. Feil</i> , 774 F.2d 1132 (Fed. Cir. 1985)	22
<i>Ortho-McNeil Pharm., Inc. v. Mylan Labs., Inc.</i> , 520 F. 3d 1358 (Fed. Cir. 2008)	23
<i>OSI Pharms., LLC v. Apotex Inc.</i> , 939 F.3d 1375 (Fed. Cir. 2019)	27
<i>Otsuka Pharm. Co. v. Sandoz, Inc.</i> , 678 F.3d 1280 (Fed. Cir. 2012)	26
<i>Randall Mfg. v. Rea</i> , 733 F.3d 1355 (Fed. Cir. 2013)	17
<i>In re Rouffet</i> , 149 F.3d 1350 (Fed. Cir. 1998)	34
<i>Samsung Elec. Co. v. Netlist, Inc.</i> , No. IPR2022-00063, Paper 53 (P.T.A.B. May 3, 2023)	32
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	8

<i>In re Wesslau</i> , 353 F.2d 238 (CCPA 1965)	27
<i>WL Gore & Assocs., Inc. v. Garlock, Inc.</i> , 721 F.2d 1540 (Fed. Cir. 1983)	22
<i>Xerox v. Bytemark</i> , No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022).....	21, 28

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Excerpts from The American Heritage Dictionary - "Firm" (4th ed. 2001)
2002	Declaration of Dr. Michael T. Goodrich in Support of Patent Owner's Response
2003	RESERVED
2004	Decision Denying Institution, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01154, Paper 11 (P.T.A.B. Jan. 24, 2022)
2005	IBM Webpage – Centripetal Networks X-Force Security, available from https://www.ibm.com/case-studies/centripetal-networks-x-force-security , dated April 12, 2022
2006	Transcript of Deposition of Douglas Jacobson, Ph.D., <i>Keysight Technologies, Inc. v. Centripetal Networks, LLC</i> , Nos. IPR2023-00445, IPR2023-00448, taken on October 2, 2023

I. INTRODUCTION

The Challenged Claims¹ are patentable over Law (Ex. 1005) because Law alone or in view of Golnabi (Ex. 1009) fails to teach or suggest a security policy management server (“SPMS”) that automatically creates or alters dynamic security policies comprising packet filtering rules that are received by the packet security gateway (“PSG”). *See generally*, ’474 Patent at Abstract, 6:10-16, 14:66-15:29, Claims 1, 9, 17, 25. Law discloses a Unified Threat Management System (“UTMS”) for high-risk or sensitive process control systems (*e.g.*, nuclear reactors) in which rulesets are initially created by operators with intimate knowledge of the process control system. *See generally*, Law at ¶¶ 22-23, 59, 90, 102. A third party with its own staff of IT personnel, firm 305, generates and sends updates to these operator-created rulesets when new threats are detected. *See id.* at ¶¶ 16, 22, 88-89. And rather than firm 305 automatically creating rules, Law discloses that IT personnel are “required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *Id.* at ¶ 16.

Law alone or in view of Golnabi also fails to teach or suggest adding, removing, or altering rules of a dynamic security policy based on a correlation

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

between portions of malicious traffic information (the “correlation” limitation). There is no dispute that Law fails to disclose the correlation limitation. Instead, Petitioner relies on the teachings of the '474 Patent itself to justify its obviousness theories, which is indicative of impermissible hindsight. See Paper 2 (“Pet.”) at 36-37 (citing the teachings of the '474 Patent). Golnabi does not cure Law's deficiency on this score because Golnabi teaches analyzing *firewall log data* generated on the protected network to adjust its rulesets, not *malicious traffic information* received at an SPMS.

Law also does not disclose nor render obvious SPMS provided rules including an indication of a feed. Petitioner's first argument, that Law discloses “rule parameters” *could* indicate a feed because they *may* be “uniquely associated” fails because (1) the plain language of the claims requires that the rules have to provide an indication of a feed, not feed-independent rule parameters and (2) Petitioner has provided no evidence that the type of information in Law's rules could possibly be used to indicate a feed. Pet. at 41-42. Petitioner's second argument, that it would be obvious to modify Law's rule table to include an indication of a feed column is conclusory and fails to explain why a POSITA would have modified the third-party firm 305 to distribute rulesets including an indication of a feed including the identifying information. Thus, Petitioner has failed to demonstrate that Law renders obvious the claimed invention.

For these reasons and those that follow, Centripetal respectfully requests the Board find the Challenged Claims patentable.

I. THE '474 PATENT OVERVIEW

The '474 Patent is directed to “[m]ethods and systems for protecting a secured network.” ’474 Patent at Abstract. Figure 1 shows a network environment having PSGs protecting networks A–D and an external security policy management server SPMS associated with the PSGs. Ex. 2002 (“Goodrich Decl.”), ¶¶ 31-33.

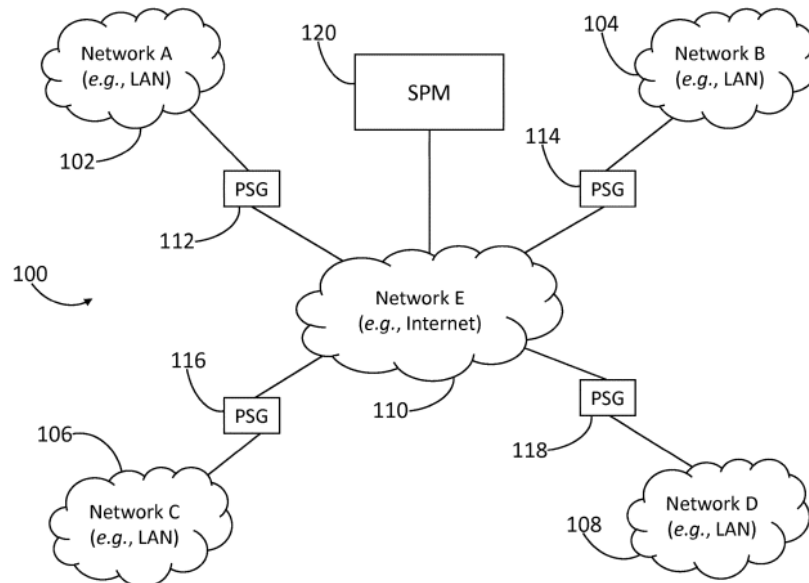


FIG. 1

'474 Patent at Fig. 1; *id.* at 4:47-55, 5:19-29.

A PSG receives from the SPMS a dynamic security policy² that includes packet matching rules having **(i)** packet matching criteria, **(ii)** corresponding packet transformation functions, and **(iii)** 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. at 1, 5, 9, Claims 1, 9, 17, 25. In the disclosed embodiments, the SPMS 120 (shown below) automatically creates dynamic security policies including rules based on malicious traffic information received from malicious host tracker services. *Id.* at 14:66-15:55.

² In one embodiment, 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.

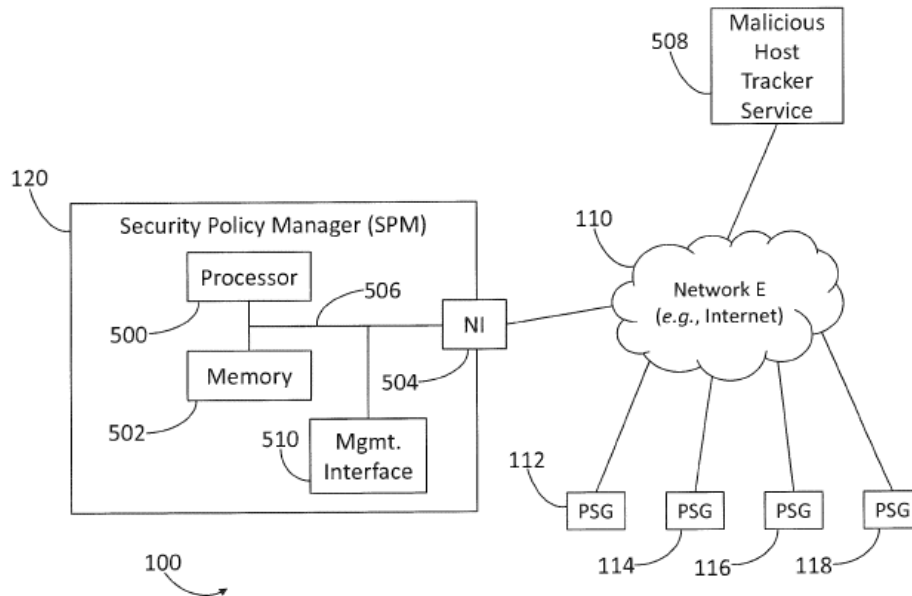


FIG. 5

Id. at Fig. 5. In this manner, the SPMS automatically creates or alters a first set of packet filtering rules of a dynamic security policy,³ and distributes the dynamic security policy to the PSGs.

³ Importantly, the SPMS's automatic creation or alteration of rules is performed without IT intervention, which differentiates traditional security systems from Centripetal's claimed security systems. Ex. 2005 at 6 ("The company's CleanINTERNET service automates threat protection This is the crux of the difference between traditional, manual security postures, and the CleanINTERNET

Further, as described and claimed in the '474 Patent, the SPMS receives security updates (*e.g.*, network addresses) from multiple malicious host tracker services as part of a subscription. *See* '474 Patent at 15:30-44 (explaining that “a network address received from host tracker service 508 may be a duplicate of a network address received from another (*e.g.*, different) service”). The SPMS correlates the updated information and may combine, remove, or alter rules of dynamic security policies associated with the correlated information. *See id.* at 15:44-57 (explaining that the SPMS “may combine the rules associated with these correlated updates”).

II. LEVEL OF ORDINARY SKILL IN THE ART

Centripetal adopts the Board's level of ordinary skill in the art set forth in its decision denying institution in IPR2021-01154, *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.* (“the '1154 decision”) challenging related U.S. Patent No. 10,785,266 (the '266 Patent”),⁴ “a person of ordinary skill in the relevant art [a “POSITA” or skilled artisan] on October 22, 2012 (the filing date of the application that matured in the '266 patent), would have had a bachelor's degree in computer

service . . . It's really cool to show traditional security stack people how this all happens without any user intervention”) (internal quotation marks omitted).

⁴ The '474 Patent is a continuation in-part of the '266 Patent.

science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack.” Ex. 2004 at 6; Goodrich Decl., ¶¶ 25-30.

III. CLAIM CONSTRUCTION

Petitioner requests that the Board adopt the constructions of the claim terms set forth in the table below that have been construed in previous IPR proceedings.

Term	The PTAB's Constructions
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 (SPMS)	a server configured to communicate a dynamic security policy to a packet gateway

See Pet. at 9-10; Goodrich Decl., ¶¶ 37-38.

The disputes in these proceedings do not turn on these constructions, and thus these constructions are not necessary. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”) (citation omitted). Nevertheless, for the purpose of this proceeding, Centripetal applies the Board’s previously adopted constructions.

IV. OVERVIEW OF THE REFERENCES

A. The Law Reference

Law is directed to an operator environment that enhances the security and management of a process control system⁵ by providing UTMS-configured devices configured and managed by operator workstations within the system. *See, e.g.*, Law at ¶¶ 22-23; Goodrich Decl., ¶¶ 39-42. Before Law, process control systems relied on firewall systems that were managed by third-party “IT personnel specifically trained to integrate the firewall into the needs of the process control system and

⁵ Process control systems are used for particularly high-risk or sensitive applications, like power generation, chemical processes, petroleum processes, nuclear reactors, high-energy processes, and/or military and government processes, which each have their own unique security requirements. *See* Law at ¶¶ 3, 15.

configure the various rulesets” Law at ¶ 16. In this regard, “separately-trained IT personnel” managed the network security while operators within the process control systems had “no capability to monitor and manage process control network security from operator workstations.” *Id.* at ¶ 21.

Law overcame the need for separately trained IT personnel with the introduction of its operator workstations that manage the UTMS-configured devices. *See id.* at ¶¶ 22-23, 59-60, 83. Specifically, the graphical displays of the workstations enable operators to create and manage rulesets (*i.e.* rulesets 147, 148, 151, and 153) specific to the unique security requirements of the system, “without IT personnel intervention.” *Id.* at ¶ 59; *see id.* at ¶¶ 23, 66, 90, 102.

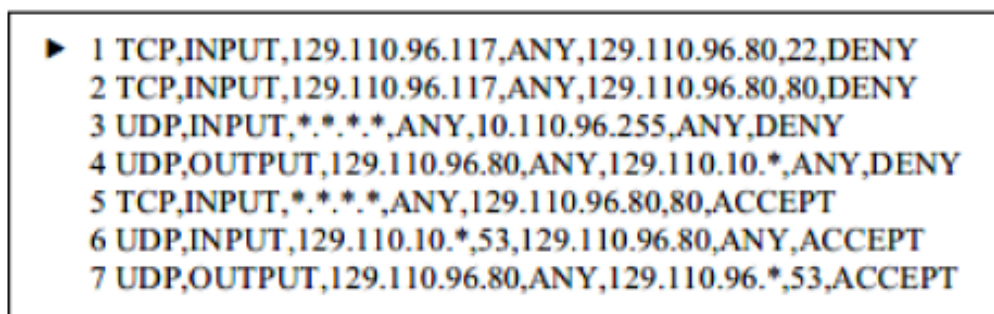
Although an operator with intimate knowledge of the process control system creates the initial rulesets, third-party IT personnel are “still required to update the ruleset when new threats are discovered or upgrades to software components of the system are implemented.” *Id.* at ¶ 88; *see also id.* at ¶¶ 16, 22, 31, 89. Law makes clear that because each operator-created ruleset is specific to the system it protects, the third-party IT personnel must “have detailed knowledge of the network architecture that is to be protected” to understand “how or why the rulesets must also be changed” to ensure that the system remains effective. Law at ¶ 16.

Accordingly, given the uniqueness of process control systems and the UTMS-configured devices, Law teaches that (i) initial rulesets are created by operators to

meet the needs of the particular process control system; and (ii) third-party IT personnel (for example of firm 305) are required to manually update the rulesets when new threats are detected. See Law at ¶¶ 16, 22-23, 88-89. On the other hand, the '474 Patent describes and claims an SPMS that automatically creates initial dynamic security policies that are received by the PSG. See '474 Patent at Claims 1, 9, 17, 25; Ex. 2005 at 6 (“The company’s CleanINTERNET service automates threat protection It’s really cool to show traditional security stack people how this all happens without any user intervention”) (internal quotation marks omitted).

B. The Golnabi Reference

Golnabi is cited for its technique of combining a group of rules. See, *e.g.*, Pet. at 38; Goodrich Decl., ¶¶ 43-44. Specifically, Golnabi discloses an aggregation technique, which combines a group of similar rules (*e.g.*, based on the same IP address 129.110.96*) into a “superset of all rules identified,” 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

Golnabi at Fig. 7; *see also id.* at 308-10, 312. To achieve this grouping, Golnabi applies the ruleset to traffic on a protected network, generates firewall log data, analyzes the firewall log data, and uses this analyzed data to combine one or more rules of the ruleset. *See id.* at 307-08 (disclosing that the process consists of extracting attributes from the firewall log data), *id.* at 312 (disclosing that the firewall log data includes packet information, including source and destination IP addresses), *id.* at 312-13 (combining rules with similar IP addresses from the firewall log data).

V. THE CHALLENGED CLAIMS ARE PATENTABLE⁶

A. Law Does Not Disclose Nor Render Obvious a Security Policy Management Server That Automatically Creates or Alters Dynamic Security Policies

The Board should confirm the patentability of the challenged claims because Law does not disclose or render obvious an SPMS that automatically generates rulesets. Goodrich Decl., ¶ 45.

⁶ In all five grounds, the Petition relies on a proposed Law-Golnabi combination set forth in Ground 1 challenging the independent claims, with Grounds 2-5 challenging the dependent claims based on the Law-Golnabi combination. *See* Pet. at 3. Accordingly, the reasons why the Challenged Claims are patentable over the proposed Law-Golnabi combination of Ground 1 apply equally to all Petition grounds.

Petitioner alleges that firm 305 is a server that automatically generates rules (or that it would have been obvious to modify firm 305 to automatically generate rulesets). See Pet. at 29-32. This allegation cannot be supported because Law expresses that: (1) firm 305 is a company that includes IT personnel and other infrastructure components; and (2) IT personnel of third-party firms, like firm 305, are still required to manually update the rulesets of process control systems. See Law at ¶¶ 16, 88-89; Goodrich Decl., ¶ 46.

1. Law Does Not Disclose the Automatic Generation of Rulesets by Firm 305

Petitioner asserts that firm 305 is a server that automatically generates rules. See Pet. at 29-31 (citing Law, ¶¶ 83, 88, and 89). But firm 305 is a company that employs IT personnel who are required to update rulesets specific to each process control system. Thus, while Petitioner alleges that firm 305 automatically constructs and distributes rulesets (*i.e.* ruleset 147) (Pet. at 29-31), Law explicitly discloses firm 305 to be a commercial entity, *e.g.*, Wurldtech Security, Inc., with IT personnel and various components involved in updating rulesets. 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.”); Goodrich Decl., ¶¶ 47-48.

During cross-examination, Dr. Jacobson testified that firm 305 is a business with various components and staff involved in updating rulesets:

So it would have to have a place to store that information

It would need then necessary processing power to work with the various -- the information that got from the 315s you have a staff to manage the infrastructure, typically these firms will also **have staff that understand, you know, something about the 315s and understand, you know, issues about threats**, et cetera. And so you're going to have some **security type personnel in the 305** and then of course that's all. You know, **I mean, I'm going to completely ignore everybody else that you need to run a business.**

Ex. 2006 (“Jacobson Tr.”) at 37:2-38:10 (emphasis added); *see also id.* at 35:11-23 (testifying that firm 305 is a service that “supplies the UTMS-configured firewalls with updated rulesets.”). In fact, Law’s paragraph 16 expressly discloses that “specifically trained” IT personnel are required to manage updates outside the operator environment when new threats are detected. *See* § V.X, *supra*; *see also* Law at ¶ 16; *see also id.* at ¶¶ 21-22, 88-89; Goodrich Decl., ¶ 49.

Accordingly, skilled artisans reading these paragraphs would understand that updating rulesets at third-party firm 305 (a commercial business) necessarily requires IT personnel involvement. Goodrich Decl., ¶ 50. Particularly, skilled artisans would have appreciated that third-party IT personnel who have detailed knowledge of the process control system are required to update rulesets when new threats are detected because they understand how and why the rulesets must be modified to protect the system. *Id.* As a concrete example, the IT personnel would

construct the updated rulesets and run tests (for example, executing computer-implemented algorithms) to ensure that the “rulesets effectively secure the process control systems in a desirable manner.” Law at ¶ 88; *see also id.* at ¶ 16; Goodrich Decl., ¶ 50.

Relying also on Law's paragraph 83, Petitioner alleges that “Law expressly discloses automatically updating (i.e., altering) rulesets” by firm 305. Pet. at 31 (citing Law at ¶ 83). That too is untrue. Critically, Petitioner misses Law's innovative feature: UTMS-configured elements of graphical displays that allow **operators** to configure and manage rulesets within the process control system. *See* Law at ¶ 83; Jacobson Tr. at 54:17-19, 55:10-56:6 (testifying that paragraph 83 is directed to the process control system). Rather than firm 305 automatically generating rules, Law's internal UTMS-configured elements implement “automatic updates” under certain network conditions. Law at ¶ 83 (detailing that the UTMS-configured elements that detect network conditions in which the graphic display elements may trigger either automatic updates or an “alarm to prompt a user to perform a manual update of the rulesets.”); Goodrich Decl., ¶ 51.

The Institution Decision's interpretation of paragraph 83 is misaligned with Law's express disclosure. Paper 7 (“Institution Decision”) at 31, 33-34. Particularly, the Decision concluded that “we disagree . . . that paragraph 83 concerns ‘the process control system, not firm 305’” because firm 305 may

continuously identify network vulnerabilities and update rulesets. *Id.* at 33-34 (citation omitted). That firm 305 continuously identifies network vulnerabilities and updates rulesets does not mean that it does so automatically, and nothing paragraph 83 says that it does. The Decision ignores the critical context that firm 305 is a service that includes separately-trained IP personnel who “are still required to update the ruleset[s]” when the updates occur outside the operator environment. Law at ¶¶ 16, 83, 88-89. In this regard, the UTMS-configured devices can receive from firm 305 the “update data” on a continuous basis, as shown in Figure 3’s “logical block diagram of a method to update rulesets of the UTMS,” but that does not mean that the “update data” was automatically generated. *Id.* at ¶¶ 30, 66, Fig. 3; Goodrich Decl., ¶ 52.

In view of the foregoing, Law does not disclose automatic generation of rulesets by firm 305. Goodrich Decl., ¶ 53.

2. Skilled Artisans Would Not Have Found it Obvious to Incorporate Automatic Generation Techniques in Firm 305 Because IT Personnel Are Required For the Updates

Petitioner asserts, in the alternative, that it would have been obvious for skilled artisans to incorporate in firm 305 the alleged automatic generation technique as referenced in paragraph 21 of Law. Pet. at 30. In making this argument, Petitioner relied on the background art for documenting what skilled artisans would allegedly be armed with when reading Law. *Id.*; Goodrich Decl., ¶ 54.

While art can be considered to show the state of the art at the time of the invention, a petitioner must “provide adequately developed explanations when relying on background knowledge based on cited art.” *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1366 (Fed. Cir. 2015). Petitioner failed to do so here. Other than saying that automatic generation was allegedly known, Petitioner does not provide any explanation or basis for how or why a skilled artisan would have ignored Law’s disclosure that trained IT personnel are “**still required to update the ruleset when new threats are discovered.**” Law at ¶ 16 (emphasis added); *see also id.* at ¶ 88 (disclosing that the third party firm provides updates to the rules “to remain effective against network threats.”).

In fact, Petitioner ignores this express disclosure that teaches away from the ’474 Patent and relied on an alleged technique without concern of how or why a POSITA would have implemented the technique in third-party firm 305. *See Chemours Co. FC, LLC v. Daikin Indus., Ltd.*, 4 F.4th 1370, 1376 (Fed. Cir. 2021) (reversing the Board’s obviousness determination because “the Board appear[ed] to have ignored the express disclosure in Kaulbach that teaches away from the claimed invention and relied on teachings from other references that were not concerned with the particular problems Kaulbach sought to solve”). As established above, firm 305 includes IT personnel who are required to update the rulesets for process control systems. *See* Law at ¶¶ 16, 88-89. Moreover, Dr. Jacobson testified that firm 305

necessarily includes “staff that understand, you know, something about the 315s and understand, you know, issues about threats,” and thus are intimately involved in the update process. Jacobson Tr. at 38:1-10; Goodrich Decl., ¶ 55.

Petitioner's failure to comply with Federal Circuit precedent as seemingly excused by the Institution Decision cannot stand scrutiny at trial because background art cannot be used to change the basis of the combination, and the alleged technique in Law does not provide state-of-the-art evidence. See Institution Decision at 31-32. **First**, the Institution Decision used the background art's alleged automatic technique to effectively supply the automatic limitation. However, background art cannot be used for the purpose of changing a petition's combinations. See *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362-63 (Fed. Cir. 2013) (emphasizing that while background art can provide evidence of the state-of-the-art, it cannot change the prior art combination that forms the basis of the asserted ground).

Here, instead of viewing the background art as evidence for what a skilled artisan would allegedly bring when reading Law's passing reference to third-party firms (*e.g.*, the cyber security risk management firm 305), the Institution Decision used the background art for supplying the alleged automatic technique. See Institution Decision at 32 (focusing on the alleged techniques disclosed in paragraph 21 of Law and a U.S. patent application publication (“the Xie publication”) for the automatic limitation). But the basis of Petitioner's proposal rested on the automatic

implementation in firm 305. In fact, the Xie publication was not even included in Petition's referenced background art. Thus, at trial, Petitioner cannot change the basis of its proposal and rely on alleged techniques in paragraph 21 of Law to supply the missing automatic generation limitation.

Second, the alleged technique in paragraph 21 does not provide state-of-the-art evidence of automatic generation by a third-party firm. During cross-examination, Dr. Jacobson admitted that he had not read the referenced cited in paragraph 21, let alone in view of firm 305 that as a business requires IT personnel to understand the threat updates. *See* Jacobson Tr. at 58:3-25; Goodrich Decl., ¶ 56. Reading paragraph 21 in view of third-party firms, a skilled artisan would appreciate that “separately-trained IT personnel” are still required to update rules to meet the needs of industrial environments they service. Goodrich Decl., ¶ 56 (citing Law at ¶ 21 (describing that “separately-trained IT personnel” are still required to “quickly and accurately manage” the industrial environment)). Similarly, in Law, separately trained IT personnel of third-party firm 305 are leveraged to update rulesets when new threats are discovered to ensure that the updates meet the needs of the particular process control system. *See, e.g.*, Law at ¶¶ 16, 88; *see also* Jacobson Tr. at 37:2-12, 38:1-10 (testifying that IT staff of firm 305 are involved in the process as they understand issues about threats). Thus, the third-party IT management referenced in paragraph 21 further supports the necessary involvement of third-party firm 305's

IT personnel when rulesets are updated to ensure that Law's process control system's needs are met. Goodrich Decl., ¶ 57.

In view of the foregoing, Petitioner cannot show that a POSITA armed with this state-of-the-art evidence would have understood that automatic generation techniques could be implemented in third-party firm 305, as the firm is not simply a server but a service that leverages IT personnel and other infrastructure components to manage updates for Law's process control systems. Goodrich Decl., ¶ 58.

* * *

At bottom, there is no rational connection between Petitioner's theory and Law's disclosure to support a finding that firm 305 employs automatic updating of rulesets. Law, therefore, does not disclose nor render obvious a security policy management server that automatically creates or alters dynamic security policies, as required by the Challenged Claims. *Id.* at ¶ 59.

B. Law in View of Golnabi Does Not Disclose Adding, Removing, or Altering Rules in a Dynamic Security Policy Based on Correlating Malicious Traffic Information

The '474 Patent discloses an SPMS that adds, removes, or alters rules of a dynamic security policy. '474 Patent at 15:30-32. To update the stored dynamic security policies, the SPMS correlates "malicious traffic information received from a plurality of malicious host tracker 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 disclosure, 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; Goodrich Decl., ¶ 60.

Petitioner acknowledges that Law does not disclose this aspect of the Challenged Claims. Pet. at 36-38. Nevertheless, Petitioner contends that this limitation would have been obvious to a POSITA in view of the conclusory *ipse dixit* testimony of its expert, Dr. Jacobson, and the ’474 Patent’s own recognition and solution to the problem. *Id.* at 37. The Board should dismiss Petitioner’s hindsight-laden approach. Goodrich Decl., ¶ 61. The Board should also determine that Golnabi does not cure Law’s deficiencies because it also fails to disclose or suggest an SPMS that correlates malicious traffic information or adding, removing, or altering packet-filtering rules based on such a correlation.

1. Law Does Not Disclose This Limitation, and the Alleged Motivation to Modify Law is the Product of Hindsight

Petitioner concedes that Law does not disclose an SPMS that adds, removes, or alters packet-filtering rules based on a correlation between portions of malicious traffic information. Pet. at 36-38. Its arguments that Law nevertheless renders this limitation obvious should be rejected as being conclusory and riven with hindsight gleaned from the ’474 Patent itself. Goodrich Decl., ¶ 62.

Firm 305 updates rules based on aggregated threat data 310 with no contemplation of removing duplicate rules. Law at ¶ 88 (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”). There is no teaching or suggestion of removing any duplicate rules, much less based on correlating threat data. Petitioner does not dispute this. Pet. at 37; Goodrich Decl., ¶ 63.

Petitioner's only record support for the assertion that Law alone renders obvious this limitation is Dr. Jacobson's conclusory, unsupported testimony, which merely parrots the Petition. See Pet. at 37 (citing Ex. 1003 at ¶ 79). Rather than citing supporting evidence or technical reason, Dr. Jacobson simply concluded that “it would have been obvious to a POSITA to analyze the received threat data 310 to remove duplicate rules.” Ex. 1003 at ¶ 79; Goodrich Decl., ¶ 64. The Board should, therefore, accord very little weight Dr. Jacobson's testimony on this point. *Xerox v. Bytemark*, No. IPR2022-00624, Paper 9 at 15-16 (P.T.A.B. Aug. 24, 2022) (precedential) (little to no weight expert testimony that “offers only a verbatim restatement of the assertion being supported, without any supporting evidence or technical reasoning”).

Rather than support his testimony with evidence that this technique was known in the art or obvious to a POSITA, Dr. Jacobson's opinion given from the opinion of one already imbued with the '474 Patent's **recognition of** and **solution to** the problem of duplicate information coming from multiple malicious host tracker services. This tactic represents impermissible hindsight. *WL Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553 (Fed. Cir. 1983) ("To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.").

Dr. Jacobson's testimony that "[i]t would have been obvious to a POSITA that there would have been a high likelihood of duplicates in the received threat data 310" (Ex. 1003 at ¶ 79) follows immediately before his recognition that "[t]he '474 Patent explains that when receiving malicious traffic information from a plurality of third party services, there may be 'duplicate[s]' in the malicious traffic information received between the plurality of services" (Ex. 1003 at ¶ 78) (citation omitted). Because there is no record evidence suggesting that this problem was known or otherwise appreciated before the '474 Patent, it is apparent that Dr. Jacobson's analysis was tainted by the hindsight gleaned from the '474 Patent itself. See *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143 (Fed. Cir. 1985) ("[T]here

must be some reason for the combination other than the hindsight gleaned from the invention itself.”) (citation omitted).

But hindsight did not only infect Dr. Jacobson's *post hoc* suggestion that a POSITA would have understood the problem associated multiple overlapping or conflicting feeds from malicious host tracker services, it also infected his analysis of what a POSITA would have done about that problem at the time of the invention. Aside from the '474 Patent itself, there is no record evidence that a POSITA would have considered solving this problem by correlating malicious traffic information at an SPMS and then adding, removing, or altering rules based on that correlation. That was the '474 Patent's solution, and Petitioner may not simply “retrace” the inventor's path and call it obvious. *See Ortho-McNeil Pharm., Inc. v. Mylan Labs., Inc.*, 520 F. 3d 1358, 1364 (Fed. Cir. 2008) (holding that it is impermissible hindsight to “simply retrace[] the path of the inventor”). Moreover, as discussed below with respect to Golnabi, POSITA were aware of **other** methods for making rulesets more efficient, and no record evidence or reasoning (other than that gleaned from the '474 Patent itself) suggests the **claimed** solution. *See* § V.A.B.2, *infra*.

Petitioner's retracing of the inventors' steps led to unexplained incongruities when considered in the context of Law's disclosure. For example, Dr. Jacobson testified that a POSITA would remove duplicate rules in ruleset 147 based on the analysis of threat data (Jacobson Tr. 23:10-24:16, Ex. 1003 at ¶ 79), but he did not

explain where those duplicate rules would have come from in the first place. Because ruleset 147 was created by the operator in the process control system, there are no duplicate rules. See Law at ¶¶ 21, 23, 81, 90 (“[T]he rulesets 148, 147, 151, 153 may be configurable by an operator or other personnel from a graphic display 129 at a workstation 120.”). Moreover, **even if** a POSITA reading Law had motivation to analyze the threat data in the first place—of which there is no evidence—the Board correctly recognized at institution that 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.” Institution Decision at 40 (quoting Prelim. Resp. at 20); Goodrich Decl., ¶¶ 64-66.

Moreover, as discussed below with respect to Golnabi, POSITA were aware of **other** methods for making rulesets more efficient, and no record evidence or reasoning (other than that gleaned from the '474 Patent itself) suggests the **claimed** solution. Accordingly, even granting Dr. Jacobson's assumption that a POSITA would have recognized the problem recognized in the '474 Patent, recognition of the problem does not make the claimed solution obvious. Goodrich Decl., ¶ 67.

Accordingly, Law alone does not teach or suggest an SPMS that correlates “malicious traffic information received from a plurality of malicious host tracker

services” or “adding, removing, or altering packet-filtering rules” based on that correlation. Goodrich Decl., ¶¶ 64-67.

2. Petitioner's Alternative Theory of Law in View of Golnabi Also Does Not Reach the Claimed Invention

Petitioner's alternative argument, that “processing the received threat data 310 to remove duplicate rules would have been obvious over Law in view of Golnabi,” also fails because a POSITA setting out to improve Law's system with Golnabi's teachings would not have reached the claimed invention. Goodrich Decl., ¶¶ 68-71.

Golnabi discloses implementing a ruleset on a protected network, running traffic through the ruleset to create firewall log data, and processing the firewall log data to find and combine similar rules. Golnabi at 314 (explaining that “our paper . . . present[s] a new process of managing firewall policy rules . . . to provide a capacity to reflect current trend of network traffic and thus to update firewall policy rules in real time from firewall log data files”). More specifically, for combining a group of similar rules, Golnabi teaches that “firewall traffic log file[s]” are processed to find attributes (such as IP addresses) for which rules are aggregated by combining a group with similar attributes (*e.g.*, 129.110.96*) from the firewall log data. *Id.* at 312 (depicting the processing steps); *see also* § V.B, *supra*.

Given that Golnabi's technique requires implementing the ruleset on a protected network and analyzing the resulting firewall logs, a POSITA seeking to

improve Law would have implemented the ruleset (as taught in Law and Golnabi) and then used resulting log data to make the ruleset more efficient. *Otsuka Pharm. Co. v. Sandoz, Inc.*, 678 F.3d 1280, 1296 (Fed. Cir. 2012) (“The inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight. What matters is the path that the person of ordinary skill in the art would have followed, as evidenced by the pertinent prior art.”) (citations omitted).

Neither Law nor Golnabi suggests correlating malicious traffic information at all, and Petitioner does not explain how or why a POSITA would have modified Golnabi’s technique to correlate malicious traffic information at an SPMS instead of simply following Golnabi’s teachings of analyzing firewall logs generated on a protected network. Petitioner has not explained *why* a POSITA to modify modified Golnabi’s teachings in order to perform correlations on Law’s threat analysis data when it could have analyzed Law’s log data instead. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.”).

Indeed, there are certain advantages to Golnabi’s technique—such as the ability to order the rules to ensure that the most frequently satisfied rules are applied first—that one gives up by shifting to the claimed solution of correlating malicious traffic information at the SPMS. Goodrich Decl., ¶ 69 (citing Golnabi at 312, 314);

Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 448 (Fed. Cir. 1986) (“It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one skilled in the art”) (quoting *In re Wesslau*, 353 F.2d 238, 241 (CCPA 1965)).

There is also no indication that Petitioner considered **how** Golnabi “generate[s] a minimum number of firewall policy rules for efficiency” (Pet. at 38) or whether a POSITA would have been able to use malicious traffic information correlations for that purpose. Accordingly, Petitioner’s allegations fail even to allege “that a person of ordinary skill in the art would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so.” *OSI Pharms., LLC v. Apotex Inc.*, 939 F.3d 1375, 1382 (Fed. Cir. 2019) (citation omitted).

Therefore, “processing the received threat data 310 to remove duplicate rules” in light of Golnabi (Pet. at 38) does not satisfy **correlating malicious traffic information** (*e.g.*, network addresses) from a plurality of malicious host tracker services and then **removing rules from the dynamic security policy** based on the correlation, as required by the Challenged Claims. See ’474 Patent at Claims 1, 9, 17, 25. Goodrich Decl., ¶ 71.

C. Law Does Not Disclose Nor Render Obvious a PSG Receiving From an SPMS a Dynamic Security Policy With Rules Including Indications of Feeds Managed by Malicious Host Tracker Services

Petitioner presents two theories, both of which fail to demonstrate that Law discloses or renders obvious SPMS provided dynamic security policies with rules having an “indication of a feed.” Goodrich Decl., ¶ 72.

Petitioner's argument that Law discloses “an indication of a feed” by rule parameters was correctly rejected by the Board that recognized packet matching criteria (rule parameters) and “an indication of a feed” are distinct components of the claimed invention. Pet. at 41-42; Institution Decision at 45-46. Rule parameters, such as “UDP, TCP, ICMP, HART, and/or SCPI,” are part of the rules that cause actions to be performed on packets if met. *See, e.g.*, '474 Patent at 7:54-59 (explaining that rules may specify IP packets containing UPD packets that cause an accept packet function to be performed); *see also id.* at 2:56-60, 8:34-44, 10:59-66; Goodrich Decl., ¶ 73.

Petitioner's conclusory statement that some sources “may have been uniquely associated with a particular combination of rule parameters” to indicate a feed lacks an evidentiary basis. Pet. at 42. Petitioner's only support comes from Dr. Jacobson who merely repeats, verbatim, the statement for which his testimony is offered to support, without any supporting evidence or technical reasoning. *Compare* Pet. at 42 (citing Ex. 1003 at ¶ 86) *with* Ex. 1003 at ¶ 86; *see also Xerox Corp. v. Bytemark*,

Inc., No. IPR2022-00624, Paper 9 at 15 (P.T.A.B. Aug. 24, 2022) (precedential) (determining that testimony of a declarant that merely repeats, verbatim, conclusory assertions from a petition, without citing additional supporting evidence or providing technical reasoning to support the testimony, is entitled to little weight).

Even more, Petitioner fails to reconcile with how a “combination of rule parameters” could even identify a particular source when various sources 315 provide the same rules and rule parameters. When addressing Law’s threat data, Dr. Jacobson testified that there is “a high likelihood of duplicates in the received threat data 310” because it is common for various sources to identify the same threats. Ex. 1003 at ¶ 79; Jacobson Tr. at 22:17-24:23 (testifying that there is a high likelihood that sources 315 identify the same threats and therefore provide the same rules including “UDP, SCPI, TCP, ICMP protocols”). Because of the high likelihood that the various sources provide the same rules, a POSITA would understand that a “combination of rule parameters” in the rules would not and could not identify particular feeds the rules come from. Goodrich Decl. at ¶¶ 73-75.

Given the foregoing, rule parameters do not provide “an indication of a feed managed by at least one of the plurality of malicious host tracker services.” Therefore, Petitioner’s argument predicated on rule parameters fails. Goodrich Decl. at ¶ 76.

Petitioner's alternative argument, that Law renders obvious "an indication of a feed" that includes an identification of a feed, fares no better. See Pet. at 42 (advancing an obviousness theory based on an interpretation referring to "identifying the feed"). The "indication of a feed" is part of a rule included in dynamic security policy rules received by the PSG from the SPMS:

receiving, by the packet security gateway and from the security policy management server, a dynamic security policy comprising packet filtering rules . . . wherein 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.

'474 Patent at Claim 1 (emphasis added); *see also id.* at Claims 9, 17. That is, by the plain reading, the SPMS provides dynamic security policy with rules having an indication of a feed. Goodrich Decl. at ¶ 77.

It is undisputed that Law does not disclose or even contemplate rules that include "an indication of a feed" that includes identifying the feed. As Law's protocol rule table 1300 (reproduced below) contains only a protocol type column, a from-address column, a threshold parameter column, a to-address column, a port number column, an action column, a description column, and log column:

1300

	1302	1304	1305	1306	1308	1310	1312	1314
	PROTOCOL	FROM	THRESH.	T0	PORT	ACTION	DESCRIPTION	LOG
1326 →	☒ UDP	10.4.0.0	n/a	232.108.1 16.118	18515	Accept	New Multicast	NO
1328 →	☐ UDP	10.8.0.0	n/a	0-7	18516	Accept	New Multicast	NO
	☐ UDP	10.8.0.0	n/a	n/a	18517	Accept	PT_COM_ RDS_IP	NO
	☐ UDP	10.8.0.0	n/a	n/a	18518	Accept	PT_COM_ RDS_IP	NO
1330 →	☒ TCP	A	< x MB/ hr	B	18519	Accept	PT_COM_ RTRP	NO
1332 →	☒ TCP	B	n/a	A	18519	Accept	PT_COM_ RTRP	NO
	☐ UDP	10.81.14.9	0-2	n/a	18520	Accept	NTP	NO
	☐ ICMP	...	...	...	18521	Accept	Remote Login	NO
	☐ ICMP	...	...	...	18522	Accept	Ping Pri-Act	NO
	☐ ICMP	...	...	...	18523	Accept	Allow SNMP Access	NO

1316	DeltaV Profile #14	LOAD	1318
1320		SAVE	1322

Fig. 13

Law at Fig. 13 (providing no “indication of a feed” column”); *see also id.* at ¶ 102. Because Law’s rule table 1300 does not include an indication column, Petitioner resorts to an obviousness theory of modifying Law’s rule table with an indication feed based on the rationale that it would helpful to a user (operator) when configuring and managing rules. Pet. at 42-43; Goodrich Decl. at ¶ 78.

However, to even entertain such a theory would require considering Law’s modified rule table in combination with the modified third-party firm 305 (the alleged SPMS end), which is missing from Petitioner’s analysis. *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016) (expressing that a single-reference obviousness theory requires that “it would have been obvious to modify that

reference to arrive at the patented invention”) (citations omitted). Particularly, Petitioner fails to provide articulated reasoning grounded in evidence for why a skilled artisan would have (or even could have) modified firm 305 to update rulesets with information indicating the sources 315 the updates are from. Without such rationale and evidence, it would not have been obvious to modify Law’s rule table with an indication of a feed column because no such information exists in the distributed ruleset updates that as stored in the rule table would indicate “the source[s] 315 upon which the rule is based.” Pet. at 43; Goodrich Decl., ¶ 79.

Where, as here, no articulated reasoning with rational underpinning supports the modification of both systems, the patent itself is used as the blueprint to arrive at the claimed invention. In *Samsung Elec. Co. v. Netlist, Inc.*, No. IPR2022-00063, Paper 53 (P.T.A.B. May 3, 2023), because both systems required modifications to arrive at the claimed invention, the Board rejected the petitioner’s obviousness theory as being impermissible influenced by hindsight. *Id.* at 33-39. Particularly, the petition relied on the distributed architecture of the Ellsberry reference as the rationale to modify the self-test module circuitry of the Jeddeloh reference, “but Ellsberry itself did not teach a testing mode.” *Id.* at 36. The Board found this to be circular, and based on hindsight. *Id.* at 36-37. Specifically, the Board reasoned that the fact Ellsberry has a distributed system does not signify to a skilled artisan, with

no knowledge of the claimed invention, to modify Jeddeloh's system and distribute the functionality into a modified Ellsberry system. *Id.*

That same logic applies here. Here, Petitioner relies on Law's rule table that enables operators to configure and control rules as the basis for modifying the table with a column including information regarding the source 315 of each rule. *See* Pet. at 42-43; Jacobson Tr. at 62:8-65:6 (testifying that his basis for the modification rested on rule table 1300 and where the data came from for trustworthiness and reliability for operators configuring rules). Significantly, when questioned where Law discloses that some sources 315 are more trustworthy or reliable than others that the identification of the sources should be communicated to operators when configuring rules, Dr. Jacobson could not point to any disclosure. Jacobson Tr. at 66:22-67:17. The fact that Law has a rule table that allows operators to configure and control rules does not signify to a skilled artisan to modify rulesets with identifying information in the third party firm 305 and distribute the rulesets into a modified Law rule table, especially when Law itself does not teach such rulesets. Goodrich Decl. at ¶ 80.

In fact, Law discloses that the UTMS-configured devices receive threat data 310 directly from sources 315 but does not teach or otherwise contemplate incorporating information regarding the source 315 to its ruleset updates and distributing the rulesets to a modified rule table. *See* Law at ¶ 92 (disclosing that the

UTMS-configured devices can “collect and aggregate threat data 310 from the firm 305 or plurality of sources 315 to construct, validate, and verify the various rulesets”); Goodrich Decl. at ¶ 81. Because Law itself does not contemplate modifying rulesets with an indication of a feed and distributing the rulesets to a modified rule table for display, there stands no articulated reasoning grounded in evidence that a skilled artisan, with no knowledge of the claimed invention, would have modified both Law and third-party firm 305 to arrive at a PSG receiving from a SPMS a dynamic security policy with rules having an indication of a feed that identifies the source. *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998) (articulating that there must be evidence that a “skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed.”).

VI. CONCLUSION

For all of these reasons, Centripetal respectfully requests that the Board hold patentable the Challenged Claims.

Respectfully submitted,

Dated: October 20, 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
Tel: (202) 824-3000 Fax: (202) 824-3001
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 RESPONSE** specified in 37 C.F.R. § 42.24 has 7,375 words in compliance with the 14,000-word limit set forth in C.F.R. § 42.24(b)(2). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: October 20, 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
Tel: (202) 824-3000 Fax: (202) 824-3001
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>	October 20, 2023
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S 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