

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

KEYSIGHT TECHNOLOGIES, INC.,  
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,  
Patent Owner.

---

Case IPR2023-00446  
U.S. Patent No. 10,567,343

---

**PATENT OWNER'S RESPONSE**

**TABLE OF CONTENTS**

|      |                                                                                                                                                                                                                                                                                  |    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I.   | INTRODUCTION .....                                                                                                                                                                                                                                                               | 1  |
| II.  | THE ’343 PATENT .....                                                                                                                                                                                                                                                            | 2  |
| A.   | Overview of the ’343 Patent.....                                                                                                                                                                                                                                                 | 2  |
| B.   | Prosecution History of the ’343 Patent .....                                                                                                                                                                                                                                     | 4  |
| C.   | Post Issuance History of the ’343 Patent.....                                                                                                                                                                                                                                    | 7  |
| III. | CLAIM CONSTRUCTION .....                                                                                                                                                                                                                                                         | 8  |
| IV.  | OVERVIEW OF THE ASSERTED REFERENCES .....                                                                                                                                                                                                                                        | 9  |
| A.   | Sourcefire .....                                                                                                                                                                                                                                                                 | 9  |
| B.   | Emerging Threats Reference .....                                                                                                                                                                                                                                                 | 9  |
| V.   | THE CHALLENGED CLAIMS ARE PATENTABLE .....                                                                                                                                                                                                                                       | 10 |
| A.   | Emerging Threats Does Not Disclose “applying ... at least one<br>packet transformation function configured to prevent an<br>exfiltration operation” Based on a Determination That an<br>Application Header Field Value Matches Second Criterion<br>Specified by an Operator..... | 13 |
| 1.   | Rule 2003021 Does Not Prevent Exfiltration Operations .....                                                                                                                                                                                                                      | 14 |
| 2.   | The Other Rules Do Not Match Any Application Layer<br>Header Field.....                                                                                                                                                                                                          | 19 |
| 3.   | Petitioner’s Cited Emerging Threats Rules Fail to Apply<br>Packet Transformation Functions “Responsive to” A<br>Determination Based on Application Packet Header .....                                                                                                           | 21 |
| B.   | Petitioner’s Obviousness Analysis is Tainted by Impermissible<br>Hindsight Bias .....                                                                                                                                                                                            | 23 |

|     |                                                                                                                                                                                                                                                                                                                                                               |    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| C.  | Petitioner Has Not Shown that Emerging Threats “Allow[s], Based on a Determination That the Application Header Field Value Indicates a Request for Specified Resource Data, Each Packet of the Second Portion of Packets Indicating a Request for Specified Resource Data to Continue Toward its Respective Destination” as Required by Claims 5 and 12 ..... | 26 |
| D.  | Evidence of Secondary Considerations Demonstrate Non-Obviousness of the Challenged Claims.....                                                                                                                                                                                                                                                                | 27 |
| 1.  | Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others .....                                                                                                                                                                                                                                                                          | 27 |
| 2.  | Industry Praise.....                                                                                                                                                                                                                                                                                                                                          | 32 |
| E.  | Emerging Threats is Not a Printed Publication.....                                                                                                                                                                                                                                                                                                            | 34 |
| 1.  | The Emerging Threats Website was Not Searchable or Meaningfully Indexed.....                                                                                                                                                                                                                                                                                  | 37 |
| 2.  | Petitioner’s Expert’s Testimony is Conclusory and Omits Key Dates and Details.....                                                                                                                                                                                                                                                                            | 40 |
| 3.  | A POSITA Would Not Have Recognized the Relevance of the Emerging Threats Reference Without the Need for Further Research or Experimentation Time.....                                                                                                                                                                                                         | 42 |
| VI. | CONCLUSION.....                                                                                                                                                                                                                                                                                                                                               | 46 |

**TABLE OF AUTHORITIES**

|                                                                                                                                  | <b>Page(s)</b> |
|----------------------------------------------------------------------------------------------------------------------------------|----------------|
| <b>Cases</b>                                                                                                                     |                |
| <i>Acceleration Bay, LLC v. Activision Blizzard Inc.</i> ,<br>908 F.3d 765 (Fed. Cir. 2018) .....                                | 35, 38, 44     |
| <i>Blue Calypso, LLC v. Groupon, Inc.</i> ,<br>815 F.3d 1331 (Fed. Cir. 2016) .....                                              | 42             |
| <i>Comair Rotron, Inc. v. Nippon Densan Corp.</i> ,<br>49 F.3d 1535 (Fed. Cir. 1995) .....                                       | 21             |
| <i>Cordis Corp. v. Boston Scientific Corp.</i> ,<br>561 F.3d 1319 (Fed. Cir. 2009) .....                                         | 42             |
| <i>In re: Cyclobenzaprine Hydrochloride Extended-Release Capsule<br/>Patent Litig.</i> ,<br>676 F.3d 1063 (Fed. Cir. 2012) ..... | 27, 28         |
| <i>Hulu, LLC v. SoundView Innovations, LLC</i> ,<br>No. IPR2018-01039, Paper 29 (P.T.A.B. Dec. 20, 2019) .....                   | 35             |
| <i>In re Klopfenstein</i> ,<br>380 F.3d 1345 (Fed. Cir. 2004) .....                                                              | 35             |
| <i>In re Lister</i> ,<br>583 F.3d 1307 (Fed. Cir. 2009) .....                                                                    | 43             |
| <i>In re Magnum Oil Tools Int'l, Ltd.</i> ,<br>829 F. 3d 1364 (Fed. Cir. 2016) .....                                             | 40             |
| <i>Millennium Pharms., Inc. v. Sandoz, Inc.</i> ,<br>862 F.3d 1356 (Fed. Cir. 2017) .....                                        | 27             |
| <i>Ortho-McNeil Pharm., Inc. v. Mylan Lab'ys, Inc.</i> ,<br>520 F.3d 1358 (Fed. Cir. 2008) .....                                 | 24             |
| <i>Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.</i> ,<br>707 F.2d 1376 (Fed. Cir. 1983) .....                        | 28             |

|                                                                                                                                    |        |
|------------------------------------------------------------------------------------------------------------------------------------|--------|
| <i>Phillips v. AWH Corp.</i> ,<br>415 F.3d 1303 (Fed. Cir. 2005) (en banc) .....                                                   | 21     |
| <i>Samsung Elecs. Co. v. Infobridge Pte. Ltd.</i> ,<br>929 F.3d 1363 (Fed. Cir. 2019) .....                                        | 35     |
| <i>In re Sponnoble</i> ,<br>405 F.2d 578 (C.C.P.A. 1969) .....                                                                     | 10     |
| <i>Valve Corp. v. Ironburg Inventions Ltd.</i> ,<br>8 F.4th 1364 (Fed. Cir. 2021) .....                                            | 35, 36 |
| <i>W.L. Gore &amp; Assocs., Inc. v. Garlock, Inc.</i> ,<br>721 F.2d 1540 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984) ..... | 23     |
| <i>In re Wyer</i> ,<br>655 F.2d 221 (C.C.P.A. 1981) .....                                                                          | 42     |
| <i>Xerox Corp. v. Bytemark, Inc.</i> ,<br>No. IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022) .....                                | 41     |
| <b>Statutes</b>                                                                                                                    |        |
| 35 U.S.C. § 102(b) .....                                                                                                           | 1      |
| 35 U.S.C. § 103 .....                                                                                                              | 5, 10  |
| 35 U.S.C. § 314(b) .....                                                                                                           | 8      |
| 35 U.S.C. § 325(d) .....                                                                                                           | 7      |

**PATENT OWNER'S EXHIBIT LIST**

| <b>Exhibit</b> | <b>Description</b>                                                                                                                                                                           |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2001           | U.S. Pat. App. Pub. No. 2012/0084866 ("Stolfo")                                                                                                                                              |
| 2002           | Petition for <i>Inter Partes</i> Review, <i>Palo Alto Networks, Inc.</i> , v. <i>Centripetal Networks, Inc.</i> , No. IPR2021-01155, Paper 2 (P.T.A.B. July 6, 2021)                         |
| 2003           | U.S. Patent No. 9,686,193                                                                                                                                                                    |
| 2004           | Decision Denying Petitioner's Request for Rehearing of Decision on Institution, <i>Cisco Sys., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2018-01559, Paper 9 (P.T.A.B. Sept. 18, 2019) |
| 2005           | Complaint for Patent Infringement, <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , No. 2:22-cv-00002, Dkt. No. 1 (E.D. Va. Jan. 1, 2022)                                  |
| 2006           | Affidavit of Service of Complaint, <i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , No. 2:22-cv-00002, Dkt. No. 14 (E.D. Va. Jan. 15, 2022)                                |
| 2007           | Opinion and Order, <i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , No. 2:18-cv-00094-HCM-LRL, Dkt. No. 621 (E.D. Va. Oct. 5, 2020)                                                |
| 2008           | Petition for <i>Inter Partes</i> Review, <i>Palo Alto Networks, Inc.</i> , v. <i>Centripetal Networks, LLC</i> , No. IPR2023-01353, Paper 3 (P.T.A.B. Sept. 5, 2023)                         |
| 2009           | Motion for Joinder to <i>Inter Partes</i> Review IPR2023-00446, <i>Palo Alto Networks, Inc.</i> , v. <i>Centripetal Networks, LLC</i> , No. IPR2023-01353, Paper 2 (P.T.A.B. Sept. 5, 2023)  |
| 2010           | Declaration of Dr. Michael Goodrich in Support of Patent Owner's Response                                                                                                                    |

| Exhibit | Description                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2011    | Transcript of the Deposition of Dr. Stuart Staniford, <i>Keysight Techs., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2023-00446 taken on October 10, 2023                                                                                                                                                                                                              |
| 2012    | Memorandum Opinion and Order regarding Claim Construction, <i>Centripetal Networks, LLC v. Palo Alto Networks, Inc.</i> , No. 21-cv-00137-EWH (E.D. Va Oct. 11, 2023)                                                                                                                                                                                                       |
| 2013    | Stack Overflow website - Linux – Directory last modified date, printed October 30, 2023                                                                                                                                                                                                                                                                                     |
| 2014    | Snort Users Manual 2.9.0. The Snort Project, March 25, 2011                                                                                                                                                                                                                                                                                                                 |
| 2015    | “Bleeding Edge Threats SID Allocation,” Emerging Threats.com archived at Internet Archive Wayback Machine on July 13, 2010 at <a href="https://web.archive.org/web/20100713225120/http://doc.emergingthreats.net/bin/view/Main/SidAllocation">https://web.archive.org/web/20100713225120/http://doc.emergingthreats.net/bin/view/Main/SidAllocation</a>                     |
| 2016    | “Emerging Threats - Ruleset Downloads,” Emerging Threats.com archived at Internet Archive Wayback Machine on July 13, 2010 at <a href="https://web.archive.org/web/20100713225532/http://doc.emergingthreats.net/bin/view/Main/AllRulesets?cover=print">https://web.archive.org/web/20100713225532/http://doc.emergingthreats.net/bin/view/Main/AllRulesets?cover=print</a> |
| 2017    | M. Jonkman. “Emerging Threats FAQs,” Emerging Threats.com. Sept. 25, 2009 archived at Internet Archive Wayback Machine on December 11, 2010 at <a href="https://web.archive.org/web/20101211164740/http://doc.emergingthreats.net:80/bin/view/Main/EmergingFAQ">https://web.archive.org/web/20101211164740/http://doc.emergingthreats.net:80/bin/view/Main/EmergingFAQ</a>  |
| 2018    | M. Jonkman. “[Bleeding-sigs] New SSL/TLS State Machine” July 5, 2006 <i>available at</i> <a href="https://marc.info/?l=bleeding-sigs&amp;m=115211167327075&amp;w=2">https://marc.info/?l=bleeding-sigs&amp;m=115211167327075&amp;w=2</a>                                                                                                                                    |
| 2019    | “[Bleeding-sigs] Bleeding Snort Daily Signature Changes,” July 6, 2006 <i>available at</i> <a href="https://marc.info/?l=bleeding-sigs&amp;m=115214763102517&amp;w=2">https://marc.info/?l=bleeding-sigs&amp;m=115214763102517&amp;w=2</a>                                                                                                                                  |

| Exhibit | Description                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2020    | "[Bleeding-sigs] Bleeding Snort Daily Signature Changes," July 10, 2006 <i>available at</i> <a href="https://marc.info/?l=bleeding-sigs&amp;m=115249327727892&amp;w=2">https://marc.info/?l=bleeding-sigs&amp;m=115249327727892&amp;w=2</a>                                                                         |
| 2021    | M. Jonkman. "Re: [Bleeding-sigs] BLEEDING-EDGE POLICY TLS/SSL Encrypted Application," May 28, 2007 <i>available at</i> <a href="https://marc.info/?l=bleeding-sigs&amp;m=118038810828100&amp;w=2">https://marc.info/?l=bleeding-sigs&amp;m=118038810828100&amp;w=2</a>                                              |
| 2022    | Commented rules – Rules – Suricata, Forum post by member of Emerging Threats rule writing team, printed October 29, 2023, <a href="https://forum.suricata.io/t/commented-rules/2283/3">https://forum.suricata.io/t/commented-rules/2283/3</a>                                                                       |
| 2023    | Data Exfiltration: How Data Gets Out, dated March 26, 2010, <i>available at</i> <a href="https://www.computerworld.com/article/2763043/data-exfiltration--how-data-gets-out.html">https://www.computerworld.com/article/2763043/data-exfiltration--how-data-gets-out.html</a>                                       |
| 2024    | Giani, A., et al., Detection of Covert Channel Encoding in Network Packet Delays, dated November 2005 <i>available at</i> <a href="https://web.archive.org/web/20100415192945/https://ists.dartmouth.edu/library/149.pdf">https://web.archive.org/web/20100415192945/https://ists.dartmouth.edu/library/149.pdf</a> |
| 2025    | Enterprise Strategy Group (ESG) White Paper - Centripetal Networks Threat Intelligence Gateway, by Tony Palmer (May 2018)                                                                                                                                                                                           |
| 2026    | American Banker Webpage – Top 10 FinTech Companies to Watch, published November 6, 2013 <a href="https://www.americanbanker.com/slideshow/top-10-fintech-companies-towatch?slide=2">https://www.americanbanker.com/slideshow/top-10-fintech-companies-towatch?slide=2</a>                                           |
| 2027    | Gartner - Cool Vendors in Security for Technology and Service Providers, 2017, published May 4, 2017                                                                                                                                                                                                                |
| 2028    | Centripetal Press Release - Centripetal Networks Named SINET 16 Innovator for 2017, dated October 31, 2017                                                                                                                                                                                                          |

| <b>Exhibit</b> | <b>Description</b>                                                                                                                                   |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2029           | Listing of Dr. Staniford's Internet Archive Wayback Machine Browsing History, provided by Petitioner's counsel for IPR2023-00446 on October 25, 2023 |
| 2030           | Internet Archive Wayback Machine - Full directory listing of Rules.emergingthreats.net, printed on October 18, 2023                                  |
| 2031           | Declaration of Pedro Marinho in Support of Patent Owner's Response                                                                                   |

## I. INTRODUCTION

Centripetal Networks, LLC, (“Centripetal” or “Patent Owner”) requests that the Board find the Challenged Claims<sup>1</sup> patentable over Sourcefire and Emerging Threats because Emerging Threats is not a printed publication under 35 U.S.C. § 102(b) and, as the Office has repeatedly confirmed, Centripetal’s exfiltration prevention methods were not only novel and non-obvious at the time of the invention, but they solved a long-felt need in the industry, received significant industry praise, and were brazenly copied by Centripetal’s competitors.

The prior administrative challenge to the ’343 Patent, and the repeated administrative challenges to its grandparent, U.S. 9,686,193 (the “’193 Patent,” Ex. 1063), all relied on Sourcefire as the primary reference. The Office has rejected each of these challenges. Based on information gleaned from these prior invalidity proceedings, Petitioner rummaged through a file of tens-of-thousands of Snort rules

---

<sup>1</sup> Keysight Technologies, Inc., (“Petitioner”) petitioned for *inter partes* review (IPR) of U.S. Patent No. 10,567,343 (Ex. 1001, the “’343 Patent”), challenging claims 1-20 (“the Challenged Claims”). On September 5, 2023, Palo Alto Networks, Inc. filed its second petition against the ’343 Patent, with a Motion for Joinder. See Exs. 2008, 2009. Palo Alto Networks’ Joinder Request is pending at time of filing this response.

for a handful that it claims are “similar” to the exfiltration prevention rules disclosed and claimed in the '343 Patent. But even with an explicit model, Petitioner could not identify a single rule that prevents exfiltration operations as claimed. In fact, the Office *already* considered each of the rules cited in the Petition, in Sourcefire, or in combination with Sourcefire during original prosecution and in earlier administrative proceedings regarding the '343 and '193 Patents.

Far from being designed to prevent exfiltration operations as claimed in these Patents, these Snort rules—plumbed from an unindexed, unadvertised website with no search functionality, which required users to navigate directories of unhelpfully-labeled folders and sub-folders—were explicitly designed for reasons *other than* exfiltration prevention and/or were turned off/commented out because they generated too many false positives to be useful. In view of these and myriad other considerations, it would not have been obvious to modify Sourcefire with any of the Emerging Threats rules identified in the Petitioner in order to prevent exfiltration operations.

## **II. THE '343 PATENT**

### **A. Overview of the '343 Patent**

The '343 Patent discloses techniques for preventing “[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet).” '343 Patent at 1:28–31; *see also* Ex. 1081 (Moore '193 Decl.), ¶ 6 (“Data

exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber-criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession.”). While exfiltrations may occur through a user’s inadvertent or accidental action, exfiltrations are often viewed as a data heist, in which malicious actors exfiltrate sensitive information, steal login credentials (usernames and passwords), and perform other forms of unauthorized data access. ’343 Patent at 2:54–58.

The inventors of the ’343 Patent recognized that exfiltrations had “proven to be especially difficult for conventional cyber defense systems to prevent.” *Id.* at 1:28–31. For example, because they are often performed on internal networks, exfiltrations appear as normal network traffic to conventional cyber defense systems. *Id.* at 1:31–36. Because users often “engage in network activities that are vulnerable to attack” and “typical network trust models . . . interpret exfiltrations as trusted operations,” such conventional cyber security systems would allow exfiltration traffic to exit the network without any remedial action being taken. *Id.* at 1:36–40.

Simply blocking communications with all untrusted computers was an unsatisfactory solution because, since the Internet is an untrusted network, such restrictions impeded legitimate access to the Internet and prevented employees from

conducting business on behalf of a company. *Id.* at 7:29–35. The '343 Patent's solution involves evaluating packet header field values, such as a Source and Destination IP address, as well as a packet transformation function which is configured to prevent an exfiltration operation. *Id.* at 7:4-9, FIG. 3. This approach allows users to “surf the web” while preventing the exfiltration of data. *Id.* at 7:9-23.

### **B. Prosecution History of the '343 Patent**

The '343 Patent issued from U.S. Patent Application No. 15/614,956 (the “'956 Application”) filed on June 6, 2017. Ex. 1002 at 29-41.

Throughout prosecution of the '956 Application, Applicant filed several Information Disclosure Statements citing documents from parallel IPR proceedings of related patents, including IPR2018-01436, challenging the validity of U.S. Patent No. 9,124,552 (the “'552 Patent”), IPR2018-01437, challenging the validity of U.S. Patent No. 9,160,713 (the “'713 Patent”), and IPR2018-01559, challenging the validity of U.S. Patent No. 9,686,193 (the “'193 Patent”): the IPR petitions, the petitioner's expert declarations in support of those petitions, and key references from both proceedings (including Sourcefire), as well as the Board's institution decision from IPR2018-01436. Ex. 1002 at 167-169 (IDS filed March 27, 2019), *id.* at 372-373, 375 (IDS filed August 8, 2018). The Examiner considered the disclosed IPR

petitions and documents (including Sourcefire) prior to issuing the Notice of Allowance. *Id.* at 127-128, 256-257, 363.

In addition to the IPR documents, Patent Owner cited a number of references that described Snort-based rules, including U.S. Pat. App. Pub. No. 2012/0240185 (“Kapoor”), U.S. Pat. App. Pub. No. 2011/0214157 (“Korsunsky”), and U.S. Patent Pub. No. 2008/0201772 (“Mondaeev”). Ex. 1002 at 62, 135. Moreover, the Office itself provided at least one reference (e.g., U.S. Pat. App. Pub. No. 2012/0084866 (“Stolfo”) (Ex. 2001)) that disclosed Snort-based rules that are substantively identical to those cited by Petitioner in Emerging Threats. Ex. 1002 at 99-117. Accordingly, the Office had Sourcefire and a multitude of other references that showed Snort-based rules throughout prosecution of the '956 Application.

Despite having the above-referenced documents and analysis from the corresponding IPRs, the Examiner rejected independent claims 1, 8, and 15 as being obvious under 35 U.S.C. § 103 over two patent references, Ahn in view of Freimuth. *Id.* at 279-307. Also, dependent claims 7, 14, and 20 were rejected as obvious over Ahn in view of Freimuth and a third reference, Buck. *Id.* at 304-305. In response to the Office Action, Applicant amended the independent claims to specify that the “at least one packet transformation function” is “configured to prevent an exfiltration operation.” *Id.* at 271, 273-274, 276. On June 3, 2019, the Examiner again rejected independent claims 1, 8, and 15, asserting the same primary reference, Ahn, but

replacing the secondary reference Freimuth with Stolfo, which shows Snort-based intrusion detection systems. *Id.* at 94-118; Ex. 2001, ¶¶ [0097], [0155].

In response to the subsequent Office Action, Applicant filed, on November 4, 2019, a Request for Continued Examination (“RCE”) with an accompanying response, amending the independent claims to recite that “the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.” Ex. 1002 at 77, 79-82. This further defined how the claimed technology is configured to prevent an exfiltration operation, while allowing other outbound traffic to continue towards its destination so that it does not unduly impede a user’s ability to surf the web. ’343 Patent, 7:3-40.

In the response, Patent Owner also explained that the prior art (i.e., Stolfo) did not teach “apply[ing], to each packet in the second portion of packets that match the second criterion, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.” Ex. 1002 at 86-88. Rather, the prior art describes “trap-based defensive mechanisms.” *Id.* at 87; Ex. 2001, ¶ [0039]. The trap-based defensive mechanisms are “used to reduce the level of system knowledge of an attacker, entice the attacker to perform actions that reveal their presence and/or identities, and

uncover and track the unauthorized activities of the attacker.” Ex. 1002 at 87-88; *see also* Ex. 2001 at ¶ [0124].

On December 12, 2019, the Examiner issued a Notice of Allowance, which included remarks that the examiner “believe[d] that the record of the prosecution as a whole does make clear the reasons for allowing claims 1-20” and to “[p]lease refer to record of prosecution.” Ex. 1002 at 35-41. The ’343 Patent then issued on February 18, 2020. ’343 Patent (Cover); Ex. 1002 at 29.

### **C. Post Issuance History of the ’343 Patent**

On March 12, 2021, the ’343 Patent was asserted against Palo Alto Networks. Ex. 1002 at 9; Ex. 2002 at 3. Palo Alto Networks filed a petition for *inter partes* review of the ’343 Patent on July 6, 2021 (IPR2021-01155). Ex. 2002 at 3. On January 1, 2022, the ’343 Patent was asserted against Petitioner. Pet. at 4. Petitioner was served with a complaint on January 6, 2022. Ex. 2006 at 3. On January 20, 2022, the Board exercised its discretion under 35 U.S.C. § 325(d) to not institute *inter partes* review of the ’343 Patent because Sourcefire, the same primary reference asserted here, was considered during prosecution of the ’343 Patent, and because Palo Alto Networks had not shown that the Examiner erred in considering Sourcefire or the other references relied upon in Palo Alto Networks’ petition against the ’343 Patent. Ex. 1077 at 2, 19-20. Keysight then filed a petition resulting in this

IPR, following the roadmap laid out in the prior PAN IPR and sought out the Emerging Threats reference from which it pulled five rules out of 11,000+.

Palo Alto Networks, now time-barred under 35 U.S.C. § 314(b), filed its second petition against the '343 Patent, with a Motion for Joinder, on September 5, 2023. *See* Exs. 2008, 2009. Palo Alto Networks' Joinder Request is pending at time of filing of this Response.

### **III. CLAIM CONSTRUCTION**

Centripetal brings to the Board's attention certain claim construction findings made in district court litigation with Palo Alto Networks ("PAN") over patent infringement of, among other patents, the '343 Patent and its continuation U.S. Patent No. 10,735,380 ("the '380 Patent). Ex. 2012 (PAN Claim Construction Order). Centripetal had argued for a plain and ordinary meaning of the terms "exfiltration," "exfiltration operation," "network exfiltration," and "network exfiltration methods" found in the '343 and '380 Patents. Ex. 2012 at 9-11. In its claim construction order, the district court adopted PAN's proposed construction of the term "network exfiltration methods" to mean "the unauthorized transfer of data from a computer by malware or by a malicious actor." *Id.* at 11; *see also id.* at 9 n.4 (acknowledging the root word "exfiltration" appears in the '343 Patent, which is subject to a partial stay in the case). Centripetal respectfully submits that Petitioner

failed to demonstrate that the asserted references render obvious the Challenged Claims under either claim construction.

#### **IV. OVERVIEW OF THE ASSERTED REFERENCES**

##### **A. Sourcefire**

Sourcefire (Ex. 1004) is a user manual titled “Sourcefire 3D System User Guide” for Version 4.10 of a Sourcefire 3D network security product. Sourcefire describes packet-filtering devices (3D Sensors) of the Sourcefire 3D System that a user may deploy in a network to passively or “inline” monitor network traffic. Ex. 1004 at 33. Each deployed 3D Sensor is capable of running an Intrusion Protection System (IPS) software component. *Id.* at 33–35. Each deployed 3D Sensor with IPS analyzes network traffic and generates intrusion events, which are records of the traffic that violate the intrusion policy applied to a detection engine on the sensor that is monitoring a specific network segment. *Id.* at 256.

Sourcefire was cited to and considered by the Examiner during prosecution of the '343 Patent. Ex. 1002 at 372, 375 (Sourcefire disclosed to Examiner in IDS filed August 8, 2018); *id.* at 362 (Examiner indicating Sourcefire was considered).

##### **B. Emerging Threats Reference**

Emerging Threats is a file containing “a copy of every rule” uploaded to the Emerging Threats website. Ex. 2016. The file contains over 11,000 rules. Ex. 1003 at ¶ 205. The Emerging Threats website purported to be “a collection point for a

number of security projects, mostly related to Intrusion Detection and network Traffic Analysis.” Ex. 2017 at 1 (the primary project concerned “the Emerging Threats Snort Ruleset contributed and maintained by the security community”). *Id.* Emerging Threats provided a number of files, and each file was associated with a particular rule category. Ex. 2016. None of these rule categories were associated with preventing exfiltrations. *See id.*; *see also* Ex. 2017 at 2-4 (describing categories of “Attack Response Rules,” “Compromised Rules,” “Policy Rules” etc.).

## **V. THE CHALLENGED CLAIMS ARE PATENTABLE**

None of the rules cited by Petitioner address the problem recognized and solved by the inventor: Preventing exfiltrations “while still preserving the flow of normal legitimate network traffic without disruption.” ’343 Patent at 7:35–40; Ex. 1085 at 112.

“[A] patentable invention may lie in the discovery of the source of a problem even though the remedy may be obvious once the source of the problem is identified. This is part of the ‘subject matter as a whole’ which should always be considered in determining the obviousness of an invention under 35 U.S.C. § 103.” *In re Sponnoble*, 405 F.2d 578, 585 (C.C.P.A. 1969). The inventor—Dr. Sean Moore—recognized that a “need for a scalable solution to the problem of exfiltration attacks was recognized by at least 2010.” Ex. 1085 at 111, ¶ 9. Dr. Moore explained that the problem addressed by the current claims was to detect and act on exfiltration

operations, “while still preserving the flow of normal legitimate network traffic without disruption.” *Id.* at 112, ¶ 11.

Petitioner and its expert frame the problem solved by the '343 Patent as preventing exfiltration operations full-stop, which ignores the very real problem of how to effectively prevent exfiltration operations without over-blocking and/or interrupting legitimate network traffic without disruption. *See, e.g.*, Pet. at 12, 24-25, 35; *see also* Ex. 1003 at ¶¶ 117-127. While many companies are using the '343 Patent's remedy in their product offerings today, it was not obvious at the time of then invention. Ex. 1085 at 112, ¶ 11 (“[P]rior attempts by others to prevent data exfiltration were often too coarse or overbroad because they would simply block all traffic to/from a given network, regardless of the actual threat, resulting in a negative impact to the subject computer network and ultimately to business operations.”).

In fact, the rules relied upon in the Petition suffer from the same, or similar, deficiencies recognized by the inventor. For example, rules that review all outgoing communications for keywords like “CONFIDENTIAL” are simultaneously overbroad (preventing attorneys from sending confidential drafts of work-product to clients) and specific (allowing the exfiltration of all data not labeled confidential). This is why many of the rules relied upon in the Petition are commented out. Ex. 1020 at 87, 109 (rules 2003021, 2002526, and 2001328 commented out).

A POSITA would have understood that Snort rules are usually commented out for having “excessive false positive” or “poor performance.” Ex. 2010 (“Goodrich Decl.”), ¶¶ 68-70; Ex. 2022 at 1 (discussing Emerging Threat staff members did not want to enable a rule and “cause sensors to potentially drop packets due to performance problems”). Dr. Staniford during this cross-examination admitted that a POSITA would have understood that the excessive false positives or negatives are significant problems and motivations when considering intrusion detection techniques. Ex. 2011 (“Staniford Tr.”) at 33:6-21 (“[I]f a product has a lot of false positives, you know, it becomes unusable”), 31:11-14 (“[I]f you block too broadly, then obviously you block a user trying to get to an asset that’s not in fact compromised”), 28:7-8, 29:20-31:8 (describing challenges and lack of accuracy in the approach of “getting lists of IP addresses and the main names of botnet controllers and detecting [them]”). Dr. Staniford also admitted that a POSITA would have understood that certain Snort rules, including Rule SID 2002526 cited by Petitioner, were “expensive” in computing resources and undesirable to run. Staniford Tr. at 68:25-69:5, 69:13-71:14 (opining that Rule SID 2002526 was commented out because it was an “expensive rule to run”).

Accordingly, Petitioner framed the problem recognized by the inventor too broadly and failed to consider the subject matter of the application as a whole by

failing to consider the need to preserve the flow of legitimate network traffic without disruption.

**A. Emerging Threats Does Not Disclose “applying ... at least one packet transformation function configured to prevent an exfiltration operation” Based on a Determination That an Application Header Field Value Matches Second Criterion Specified by an Operator**

Petitioner has not met its burden to show that Sourcefire in view of Emerging Threats discloses “applying... at least one packet transformation function configured to prevent an exfiltration operation” or that it would have been obvious to modify Sourcefire with Emerging Threats to reach the Challenged Claims.

Recognizing that numerous prior proceedings found that Sourcefire does not disclose or suggest rules for preventing exfiltration operations (Pet. at 12-16), Petitioner alleges that “Emerging Threats discloses such operators that perform the same exfiltration protection disclosed and claimed in the '343 patent.” Pet. at 23 (citing Ex. 1003, ¶ 150). Specifically, the Petition refers to a number of rules that are purportedly related to the claims. Pet. at 37-43 (citing rule SIDs 2002526, 2002034, 2001328, 2003021), 54 (citing rule 2003021), 56-61 (same), 61-62 (citing rule SID 2005319), 67 (citing rule SID 2003326); *see also* Ex. 1003 at ¶ 159 (citing rule SID 2006409), ¶ 194 (citing rule SID 2007820), ¶ 200 (citing rule SID 2001022), ¶ 282 (citing rule SID 2010234). Petitioner does not show that any of these rules prevent exfiltrations or that the rules prevent exfiltrations based on an

application header field value matching a criterion specified by an operator, as claimed.

Although the Petition cites to various rules in the Emerging Threats reference as prior art to the Challenge Claims, the Board, in its Institution Decision, narrowed its analysis with respect to limitation 1[e] and the Emerging Threats rule having SID 2003021 ("Rule 2003021"). DI at 31 (finding "immaterial" Centripetal's counterarguments about other Emerging Threats rules raised by Petitioner). That Rule, discussed below, is not configured to preventing an exfiltration operation. To the extent Petitioner attempts to shift its argument to other rules in the Emerging Threats reference, Petitioner should be barred from doing so.

### **1. Rule 2003021 Does Not Prevent Exfiltration Operations**

The Rule 2003021 does not prevent exfiltration operations.

#Application data stream

#

#alert tcp \$HOME\_NET any -> \$EXTERNAL\_NET 1024:65535 (msg:"ET  
POLICY TLS/SSL Encrypted Application Data on Unusual Port SSLv3";  
flowbits:isset,BS.SSL.Established; flow:established,to\_server; content:"|17  
03 00|"; depth:4; threshold:typelimit, count 1, seconds 120, track by\_src;  
classtype:unusual-client-port-connection;  
reference:url,doc.emergingthreats.net/2003021;  
reference:url,www.emergingthreats.net/cgi-

bin/cvswb.cgi/sigs/POLICY/POLICY\_SSL\_TLS\_on\_High\_Port;  
sid:2003021; rev:8;)

Ex. 1020 at 109.

First and foremost, this rule cannot prevent exfiltration operations because it is not only merely an “alert” rule, which cannot block traffic, it is commented out. Rules that are commented out are not applied to packets at all and cannot, therefore, prevent exfiltration operations. Furthermore, Petitioner has not established that it would be obvious to either uncomment this rule or to change it from an alert rule to a block rule such that it would prevent an exfiltration operation, as claimed. See § V.B, *infra*.

In any event, a POSITA would not recognize Rule 2003021 as a “rule configured to prevent an exfiltration operation by detecting attempts to transmit traffic to unusual ports using an out-of-date and insecure encryption protocol.” Pet. at 57; *see also id.* at 40, 54; Goodrich Decl., ¶¶ 76-80. Petitioner’s assertion about the purpose and operation of this rule is supported only by Dr. Staniford’s conclusory, *ipse dixit* testimony in an attempt to fill in limitations admittedly unmet in Sourcefire. The rule itself, and contemporaneous evidence about the rule, lead to a different conclusion.

The plain language of the Rule 2003021 indicates that the rule is not configured to prevent exfiltration operations. Goodrich Decl., ¶ 77. First, the plain

language of the Rule 2003021 says nothing about “exfiltration.” Ex. 1020 at 109. During cross-examination, Petitioner’s expert acknowledged that the message parameter in Snort rules are a strong indication of the intended purpose of the Snort rule. Staniford Tr. at 88:5-10 (“The message is ... intended to give the user some suggestion of the point of the rule”). Here, the message parameter of Rule 2003021 indicates that the rule is intended to target encrypted traffic having an “Unusual Port,” and says nothing about exfiltration. Ex. 1020 at 109 (“msg: ‘ET POLICY TLS/SSL Encrypted Application Data on Unusual Port SSLv3’”). This is consistent with the other parameters in the rule, which indicate the classification type of the rule is for unusual client port connections (“classtype: unusual-client-port-connection;”), and category of rule is for policies with SSL/TLS on high ports (“POLICY\_SSL\_TLS\_on\_High\_Port”). Goodrich Decl., ¶ 77.

Rule 2003021 was not created to prevent exfiltration operation; it was created to capture traffic from a particular new bot that generated encrypted traffic on a high port. Goodrich Decl., ¶ 78. Ex. 2018 at 1 (“The impetus to create [these rules] was a new bot that’s using standard ssl for a command and control session on a high port.”). A POSITA would have understood that Rule SID: 2003021 is one of a string of signatures designed to identify good SSL or TLS sessions at high ports (e.g., >1023). Ex. 2018; *see also* Ex. 2019.

That the goal of this rule was to catch a particular bot, not prevent an exfiltration operation, becomes readily apparent when rule SID 2003021 is read in context with other rules in the same ruleset. For example, rule SID: 2003026 does *not* generate an alert for SSL traffic on port 443, regardless of which version of SSL is used. Ex. 1020 at 107. Rule SID: 2004598 excludes SSL traffic associated with America Online from generating SSL alerts, regardless of the version of SSL and/or TLS being used. *Id.* Similar rules prevent alerts for SSL traffic—regardless of the version of SSL being used—on a variety of other ports, including port 8000, 8080, 8200, 8443, 5222, 5223, 2967, 3128, 8292, 8294, 1521 and 995. *Id.* at 107-108 (e.g., SID 2003027, SID 2003028, SID 2003029, SID 2003030, SID 2003031, SID 2003032, SID 2003033, SID 2003035, SID 2003036, SID 2003037, SID 2003038, SID 2003934, SID 2008543).

Thus, the rule identified by SID 2003021 was designed to flag certain SSL traffic on high ports while attempting to capture a bot, not to prevent exfiltration operations. Goodrich Decl., ¶ 80. This evidence about the purpose and operation of rule SID 2003021 contradicts Dr. Staniford's testimony that "this rule was not directed to looking for instances of exploits or attacks . . . ." Ex. 1003 at ¶ 228. To the contrary, rule SID 2003021, ham-handedly attempts to identify a particular bot with a *very* broad net that captures so much legitimate traffic that many, many other rules were needed to patch its overbreadth.

In its Institution Decision, the Board credited a correspondence made between the REQUIRE-TLS-1.1-1.2 operator in the '343 Patent and the Rule SID 2003021 in the Emerging Threats reference. DI at 32. However, there is no evidence to support a conclusion that Rule SID 2003021 prevents exfiltration operations by capturing encrypted traffic on “high ports” while allowing it on other ports. Goodrich Decl., ¶ 81. Indeed, there is no evidence in the record showing a correlation between high ports and exfiltration operations. *See also* Staniford Tr. 97:4-16 (Petitioner's expert admitting neither the comment or the message parameter of Rule SID 2003021 say anything about exfiltration); *id.* at 103:22-104:6 (failing to remember having seen or remarked on any such evidence in his declaration). In fact, all that is needed to defeat this rule (if it were not commented out to begin with) is to send data over a standard SSL port instead of a high port.

And while the Board credited Dr. Staniford's recollection of “working on a similar feature where we looked for large encrypted transmissions outbound from the network on non-HTTP ports as a possible symptom of exfiltration of large amounts of data,” there is no evidence, contemporaneous or otherwise, supporting his statement. DI at 32-33 (quoting Ex. 1003 at ¶ 228). Indeed, during cross-examination, Dr. Staniford revealed his feature was targeted at the size of the outgoing encrypted transmissions, rather than any high port numbers or SSL version. Staniford Tr. at 93:8 (“large encrypted transmission”), 94:2-6 (“[the CEO]

wanted to have as a feature **large** encrypted transmissions”, “if we saw a **big chunk** of encrypted data going out”) (emphasis added); Goodrich Decl., ¶ 82 (citing also Staniford Tr. at 92:10-97:3, 102:5-103:21).

## **2. The Other Rules Do Not Match Any Application Layer Header Field**

The Board acknowledged that the Petitioner has not argued that any other rules are applicable to this limitation, and therefore are not part of Petitioner's case. DI at 31. To the extent that Petitioner disagrees, Patent Owner reiterates several reasons why the three rules mentioned in the Petition do not meet the claim limitations.

One rule (i.e., SID: 2002526) “searches for markings [e.g., ‘TOP SECRET,’ ‘TS,’ or ‘NOFORN’] in HTTP content flowing toward external servers indicating that the information was classified as top secret and not for distribution to foreign nationals.” Pet. at 39. A second rule (i.e., SID: 2002034) is “configured to detect and block unauthorized transmission of the password file from Unix/Linux systems” by “search[ing] for the beginning of the first line of a Unix/Linux password file.” *Id.* at 40. The third rule (i.e., SID: 2001328) describes blocking “application layer information containing social security numbers with the familiar ‘-XX-XXXX’ ending pattern.” *Id.* However, these rules merely match strings of characters and do not analyze the *an application header field* value, as required by the claims. Goodrich Decl., ¶ 84.

To the extent Petitioner argues that “the Board found in the ’552 IPR that Sourcefire discloses applying an operator that specifies one or more application-header-field-value criteria and a packet transformation function,” Petitioner fails to explain how the three rules above would be combined with the operator the Board previously found in the ’552 Patent IPR. Pet. at 58. These three rules are explicitly crafted to alert an administrator when strings are matched. Petitioner does not explain why a POSITA would have imported these rules into Sourcefire and then modified them to *also* target an “application header field value,” as claimed. The unaccounted for modifications to these rules would alter the “principle of operation” behind them, without Petitioner having explained what would have motivated a POSITA to make such a modification.

Issue preclusion does not bar Patent Owner’s arguments that the combination of Sourcefire and Emerging Threats do not disclose or suggest an operator that specifies one or more application header field value criteria. *Id.* at 45 (“[T]he finding[] that Sourcefire . . . teaches materially similar elements of the ’552 patent claims are binding here.”); *id.* at 58. The standard for finding collateral estoppel is strict and requires the identical issues to be decided in the first action:

[1] that in the prior action the party against whom estoppel is sought had a full and fair opportunity to litigate the issue; [2] the issue was actually litigated; [3] the controlling facts and applicable legal rules were the same in both actions; [4] resolution of the particular issue was

essential to the final judgment in the first action; and [5] the identical issue was decided in the first action.

*Comair Rotron, Inc. v. Nippon Densan Corp.*, 49 F.3d 1535, 1537 (Fed. Cir. 1995) (citations omitted). Because the '552 Patent does not recite at least “determining, based on an application header field value, the second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule,” the issue of whether Sourcefire discloses determining whether an application header field value matches second criterion specified by an operator was not (and could not have been) litigated in IPR2018-01436. The applicable legal rules are also not the same because the Board applied the broadest reasonable interpretation (“BRI”) standard in IPR2018-01436 whereas it applies the *Phillips* standard here. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

**3. Petitioner's Cited Emerging Threats Rules Fail to Apply Packet Transformation Functions “Responsive to” A Determination Based on Application Packet Header**

Emerging Threats also fails to render obvious the Challenged Claims because none of its rules, particularly the rules cited by Petitioner, prevent exfiltration operations ***responsive to*** “determining, based on an application header field value” the first portion of packets corresponds to the claimed one or more operators’ second criterion. Goodrich Decl., ¶¶ 86-89.

The '343 Patent discloses and claims preventing an exfiltration operation “**responsive to** determining the second portion of packets that comprises data corresponding to the second criterion,” which is “an application header field value.” '343 Patent at Claims 1, 8, and 15 (emphasis added). In accordance with this limitation, the specification of the '343 Patent provides examples where the system inspects packets for a matching application layer header value (*i.e.* GET, POST, PUT, etc.), and performs a packet transformation function (*i.e.* ALLOW or BLOCK):

```
Operator HTTP-EXFIL(ip-packet):  
Inspect app-pkt(ip-packet) match GET return ALLOW;  
Inspect app-pkt(ip-packet) match POST return BLOCK; 55  
Inspect app-pkt(ip-packet) match PUT return BLOCK;  
Inspect app-pkt(ip-packet) match DELETE return  
BLOCK;  
Inspect app-pkt(ip-packet) match CONNECT return  
BLOCK; 60  
Return BLOCK;  
End Operator HTTP-EXFIL;
```

'343 Patent at 7:53-62.

On the other hand, no rule in Emerging Threats is written to trigger based on the application layer header field. For example, in the case of Rule SID 2002526, the rule provides a regular expression (*i.e.*, “pcre:”/(TOP{\sSECRET|TS})//[\s\w,\-...”) which does not analyze the “application packet header field value.” Goodrich Decl., ¶ 88. In another example, in the case of Rule SID 2002034, the rule specifies

payload content that appears similar to an /etc/passwd file but does not analyze any application header field value. Goodrich Decl., ¶ 89. Thus, these rules simply do not prevent an exfiltration operation or analyze any application layer header field values.

**B. Petitioner's Obviousness Analysis is Tainted by Impermissible Hindsight Bias**

Petitioner's reliance on Emerging Threats (Ex. 1020) is based on impermissible hindsight gleaned from Patent Owner's disclosure, as well as prior invalidity proceedings against the parent (e.g., U.S. 9,160,713) (Ex. 1068), grandparent (e.g., U.S. 9,686,193) (Ex. 1070), and great-grandparent (e.g., U.S. 9,124,552) patents (Ex. 1067).

Petitioner's analysis is tainted by hindsight bias because Petitioner distilled the invention down to its "gist" or "thrust," disregarding the requirement of analyzing the subject matter "as a whole." *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1548, 1553 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984).

In doing so, Petitioner has failed to address the source of the problem with preventing exfiltration operations. The inventor did not only devise a technique for preventing exfiltrations, he devised a technique that prevented exfiltrations without completely hampering the user's ability to surf the web. The Petition completely missed this point. Additionally, no POSITA would implement a rule to prevent exfiltration operations when (1) there was no indication that anyone was aware of its

applicability to exfiltration operations or (2) the rule was commented out, like Emerging Threats Rule SID 2003021. Ex. 2031 (Marinho Decl.), ¶¶ 7-21 (former Emerging Threats employee discussing applicability of asserted rules to preventing exfiltration operation).

Petitioner's obviousness theory in this case did nothing more than retrace the path of the inventor, using the application header field values identified in the specification in an attempt to find similar rules. *Ortho-McNeil Pharm., Inc. v. Mylan Lab'ys, Inc.*, 520 F.3d 1358, 1364 (Fed. Cir. 2008) (discounting an expert's testimony as "simply retrac[ing] the path of the inventor with hindsight" as "always inappropriate for an obviousness test . . ."). As noted above, the author of rule SID: 2003021, Matt Jonkman, indicated that "[t]he impetus to create [these rules] was a new bot that's using standard ssl for a command and control session on a high port." Ex. 2018 at 1. Without the guidance provided by the disclosure of the '343 Patent and the operators described therein, a POSITA, exercising reasonable diligence, would not have recognized the relevance of rule SID: 2003021 to exfiltration prevention. Indeed, this rule was not recognized *at the time* to have anything to do with exfiltration prevention. Accordingly, Petitioner's reliance on Emerging Threats (Ex. 1020) is based on impermissible hindsight gleaned from Patent Owner's disclosure.

Petitioner's hindsight bias is further demonstrated by its use of evidence dated *after* the time of invention to support its theory that a skilled artisan would have applied the Emerging Threats reference to render obvious the Challenged Claims. Pet. at 37; Ex. 1003 at ¶¶ 232-233. Petitioner uses an antedated Centripetal press release (Ex. 1082) and argues that "Patent Owner's press release touted that the Emerging Threats rulesets are 'platform agnostic' for easy integration with SNORT and other network intrusion protection and detection systems." Pet. at 37 (citing Ex. 1082). But, Petitioner ignores its evidence's key flaw: the Centripetal press release appears to be dated "August 19, 2014", which is four years after the alleged December 2, 2010 publication date of the Emerging Threats reference and well after the effective filing date of the '343 Patent. Ex. 1082 at 1; *see also* Staniford Tr. at 46:19-25 (Dr. Staniford acknowledging during cross-examination that this evidence antedates the priority date of the '343 Patent). The Centripetal press release cannot be used to hold up Petitioner's theory that it would have been obvious to a skilled artisan to apply the Emerging Threats reference with Sourcefire to reach the Challenged Claims *at the time of the invention*.

Also, while the Centripetal press release characterizes the Emerging Threats project as being originally "[f]ounded in 2003 as a cyber security research community," the press release is silent as to when the project allegedly became known as the "de facto standard in network-based malware threat detection." Ex.

1082 at 2. Because the Centripetal press release post-dates the '343 Patent and is silent on key dates about Emerging Threat's alleged popularity, its mention of the Emerging Threats project provides little insight into whether it would have been obvious to a POSITA to apply the Emerging Threat reference to Sourcefire at the critical time period.

Because Petitioner's purported showing of obviousness is unsupported by any knowledge that was within the level of ordinary skill at the time the claimed invention was made, and instead relies on knowledge gleaned from the '343 Patent's disclosure and prior invalidity proceedings, Petitioner's analysis is impermissibly tainted by hindsight bias and should be rejected. Goodrich Decl., ¶¶ 90-96, 93 (discussing Ex. 1019).

**C. Petitioner Has Not Shown that Emerging Threats “Allow[s], Based on a Determination That the Application Header Field Value Indicates a Request for Specified Resource Data, Each Packet of the Second Portion of Packets Indicating a Request for Specified Resource Data to Continue Toward its Respective Destination” as Required by Claims 5 and 12**

Petitioner argues that claims 5 and 12 are taught by Emerging Threats rule SID: 2010234. Pet. at 64-66. However, Petitioner fails to identify any analysis of application header field values.

Petitioner's rationale and motivation to modify the rule is another of example of cherry-picking various rules and fine tuning them based on whatever modifications are necessary to reach the challenged claims rather than being guided

by the teachings of the prior art and the understandings of a POSITA at the time of the invention. This is further evidence of Petitioner's use of impermissible hindsight, as discussed in Section V.B, and highlights the Petitioner's shortcomings in showing that Emerging Threats discloses "allowing, based on a determination that the application header field value indicates a request for specified resource data, each packet of the second portion of packets indicating a request for specified resource data to continue toward its respective destination."

**D. Evidence of Secondary Considerations Demonstrate Non-Obviousness of the Challenged Claims**

In addition to the reasons above, objective evidence demonstrates that Challenged Claims are not obvious. Evidence of objective indicia "can be the most probative evidence of nonobviousness in the record," and objective indicia enable "the court to avert the trap of hindsight." *Millennium Pharms., Inc. v. Sandoz, Inc.*, 862 F.3d 1356, 1367-68 (Fed. Cir. 2017) (citations omitted).

Petitioner's expert admitted during cross-examination that he did not consider any evidence of secondary considerations when forming his opinions about the validity of the Challenged Claims. Staniford Tr. at 151:19-152:18.

**1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others**

The failure of others can result in a strong indication of non-obviousness. See *In re: Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676

F.3d 1063, 1075, 1081-83 (Fed. Cir. 2012) (reversing district court and finding evidence of unexpected results and long-felt need for those results supported a finding of non-obviousness). Failure of others is also indicative of unexpected results and long-felt need because one of ordinary skill in the art would not reasonably expect the success. *See id*; *see also Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1382 (Fed. Cir. 1983) (holding that the lack of previous attempts to achieve the results of the invention indicated a lack of long-felt need).

The '343 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to protect against “[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet).” Goodrich Decl., ¶ 104 (citing '343 Patent at 1:28-51). Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession. Goodrich Decl., ¶ 104 (citing Ex. 2023, Ex. 2024).

This problem has been known in the industry since at least 2006, and while it was extensively discussed in research papers and trade periodicals, it was still an ongoing problem. Goodrich Decl., ¶ 105 (citing Ex. 2023 and Ex. 2024).

Centripetal solved this long-felt, unsolved need with its RuleGATE, Advanced Cyber Threat, and QuickTHREAT system components, which practices the '343 Patent. Goodrich Decl., ¶ 105.

Centripetal's solution to this long-felt problem began with the recognition that exfiltrations can be facilitated by using various protocols, such as the Hypertext Transfer Protocol (HTTP). Goodrich Decl., ¶ 106. Because bad actors on the internet discovered that they could exfiltrate valuable data using popular protocols rather than explicitly malicious code, traditional signature-based techniques designed to recognize and prevent the transfer of malicious code into a network were not suited to stopping the emerging exfiltration problem. *Id.* Further, because exfiltrations are mediated by popular data transfer protocols, it was also not an option simply to block all traffic utilizing a particular protocol, even when those protocols had a known vulnerability. Goodrich Decl., ¶ 106.

The claims of the '343 Patent recite techniques that address this long-felt but unresolved problem of data exfiltrations. The claims of the '343 Patent involve applying "packet-filtering rules" specifically crafted to prevent such exfiltrations. Goodrich Decl., ¶ 107. In particular, the claimed invention prevents malicious exfiltrations by (1) processing packets looking for a "first criterion" on "packet header field value," and a "second criterion" based on an "application header field value," and (2) applying a packet transformation function "configured to prevent an

exfiltration operation,” as claimed. *See* '343 Patent, Claim 1. The claims of the '343 Patent are embodied in Centripetal's CleanINTERNET and RuleGATE products. The RuleGATE and CleanINTERNET products include the ability to counter these types of exfiltrations and also address insider threats. Goodrich Decl., ¶ 107.

Centripetal's solution to these problems greatly curtailed the risk of data exfiltration by detecting the threat earlier and acting in response while still preserving the flow of normal network traffic without disruption. In particular, Centripetal recognized that it could employ cyber-threat intelligence (“CTI”) to focus its data-transfer-method-based packet filtering on traffic destined for potentially risky hosts on the Internet. Goodrich Decl., ¶ 108. This process succeeded where traditional, overbroad techniques failed because it permitted normal business network traffic, like allowing a web browser to download web pages hosted by web servers, while still preventing data exfiltrations. Goodrich Decl., ¶ 108.

Prior attempts by others to prevent data exfiltration were often too coarse or overbroad (such as blocking all HTTP traffic), resulting in negative impact to the subject computer network and ultimately to business operations. Goodrich Decl., ¶ 109. But using Centripetal's technique in conjunction with CTI, the '343 Patent could allow packets based on its packet header field values and specify additional precautions for other packets. *Id.*; Goodrich Decl., ¶ 109.

Centripetal's inventions unlocked the ability to derive network threat intelligence data (from multiple sources) and "operationalize" cyber threat intelligence (CTI) to proactively protect networks. The claimed invention leveraged CTI by applying operators ("applying... one or more operators specified by the at least one matching packet-filtering rule") to only those packets meeting specified packet header criteria ("responsive to a determination by the computing system that a packet header field value of the first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule") rather than blocking any and all outgoing traffic utilizing a particular protocol (*e.g.*, HTTP). Goodrich Decl., ¶ 110. The '343 Patent provides the example of "an HTTP-EXFIL operator" that "may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (*e.g.*, PUT, POST, CONNECT, *etc.*)."' '343 Patent at 7:9-13, 7:52-62.

The '343 Patent explains that the exemplary HTTP-EXFIL operator achieves the solution of stopping exfiltrations "[b]ecause attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data." '343 Patent at 7:21-23. The '343 Patent also explains that this process succeeds where traditional, overbroad techniques failed because it enables, for example, the operator to "thus allow a web browser to 'surf the web' (*e.g.*, download web pages hosted by web servers), but [] prevent the web browser from writing files to a web server (*e.g.*, using the PUT

method), posting forms (e.g., forms that might contain login credentials, such as usernames or passwords) to a web server (e.g., using the POST method), or otherwise communicating with a web server (e.g., using any HTTP method except GET).” ’343 Patent at 7:13-21; Goodrich Decl., ¶¶ 111-12.

Centripetal’s solution to the exfiltration solved the long-standing problem of how to prevent exfiltrations that are mediated by popular protocols, demonstrating the nonobviousness of the ’343 Patent Claims.

## **2. Industry Praise**

Products embodying the invention claimed in the ’343 Patent have received substantial industry praise. Goodrich Decl., ¶¶ 114-117. In a white paper entitled “Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement,” an industry research firm named ESG Research praised Centripetal’s Threat Intelligence Gateway as having “the highest performance network filter that ESG has tested or seen in action to date.” Ex. 2025 at 8; Goodrich Decl., ¶ 114. The ESG Paper further lauded Centripetal’s Threat Intelligence Gateway’s ability to “deliver[] more than is possible with firewalls and IPS systems,” pointing to Centripetal’s RuleGATE and CleanINTERNET products. Ex. 2025 at 7.

The Security Innovation Network (“SINET”) named Centripetal the SINET 16 Innovator for 2017 at the SINET Showcase in Washington D.C. See Ex. 2028.

This award praises Centripetal's CleanINTERNET solution which "can persistently prevent over 90% of known threats with applied threat intelligence, rapid correlation, and automated enforcement of millions of IOC policies against live network traffic with live cyber analyst support." *Id.* at 2. It further offered praise, stating that "SINET sees the true innovation in what Centripetal is bringing to market by way of operationalizing threat intelligence for any size company for real-time, intelligence-led protection." *Id.* at 1. This award is tied to the technologies in the '343 Patent because they provide techniques for preventing malicious exfiltration. Goodrich Decl., ¶ 115.

Centripetal was recognized as an innovator by trade periodicals and analysts. On May 4, 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers," praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2027 at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id.* Centripetal Networks was also named one of American Banker's "Top 10 FinTech Companies to Watch" for 2014 because its Threat Intelligence Gateway, RuleGATE

“has the potential to detect and deter rapidly changing cybersecurity threats on the fly.” Ex. 2026 at 11; Goodrich Decl., ¶ 116.

The evidence of industry praise discussed above is reasonably commensurate with the scope of the claims of the '343 Patent and that there is a nexus between the merits of the claimed invention and the evidence of secondary considerations, as the praise is directed at Centripetal's products which embody the claimed features of the '343 Patent. Therefore, the praise that Centripetal's products and technology have received from others further demonstrates that the claimed invention of the '343 Patent is not obvious.

**E. Emerging Threats is Not a Printed Publication**

Petitioner has failed to show that a POSITA, exercising reasonable diligence, would have been able to locate the Emerging Threats reference (Ex. 1020) on the alleged date of December 2, 2010 (Pet. at 18) or before the March 12, 2013, effective filing date of the '343 Patent.<sup>2</sup> Moreover, Petitioner has failed to show that a POSITA would be able to recognize the relevance of the Emerging Threats reference without the need for further research or experimentation.

---

<sup>2</sup> Petitioner does not dispute that the effective filing date of the '343 Patent is March 12, 2013. Pet. at 12; '343 Patent at code (63).

The determination of whether a reference is a “printed publication” is a “case-by-case inquiry into the facts and circumstances surrounding the reference’s disclosure to members of the public.” *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004) (citations omitted). In Petitioner’s view, the fact that the Wayback Machine archived a copy of the Emerging Threats reference is dispositive. Pet. at 18-19. This is incorrect. Petitioner mistakes technical accessibility for public accessibility.

While the existence of a Wayback Machine archive might mean the Emerging Threats reference was technically accessible (*i.e.*, someone could “theoretically find it on the Internet”), “[p]ublic accessibility requires more than technical accessibility.” *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019) (citation omitted); *Hulu, LLC v. SoundView Innovations, LLC*, No. IPR2018-01039, Paper 29 at 10 (P.T.A.B. Dec. 20, 2019) (citing *Samsung Elecs.*, 929 F.3d at 1369). A reference is publicly accessible only if it was “disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.” *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (citations omitted).

The *Valve Corp.* decision cited in the Petition is instructive. In *Valve Corp.*, the Federal Circuit concluded that there was “overwhelming evidence” of public

accessibility of a prior art article in the form of (1) testimony from the inventor and (2) evidence that the patent examiners, who are “trained and required to determine publication dates,” concluded that the article was “published” two years before the priority date. *Valve Corp. v. Ironburg Inventions Ltd.*, 8 F.4th 1364, 1373-74 (Fed. Cir. 2021) (citation omitted). The Court then used the Wayback Machine evidence to corroborate the publication date, not to suggest that the mere existence of a document on the Internet as of a certain date was evidence of public accessibility. *Id.* at 1374-75. In the present case, there is no such testimony or determination by an examiner in the record.

Petitioner also cites two cases in support of its mistaken contention that “[t]he Internet Archive’s Wayback Machine shows the public accessibility of Emerging Threats.” Pet. at 18 (citing *Veeam Software Corp. v. Symantec Corp.*, No. IPR2013-00142, Paper 11 at 9-10 (P.T.A.B. Aug. 7, 2013) and *Pohl v. Mh Sub I, LLC*, 332 F.R.D. 713, 717-18 (N.D. Fla. 2019)). But like *Valve Corp.*, these cases do not stand for Petitioner’s proposition. Instead, they further support the conclusion that the Wayback Machine can provide evidence relevant to authenticity of exhibits and technical accessibility, not public accessibility.

Additionally, the record evidence of this case shows the Emerging Threats reference was not publicly accessibly because it was buried on a website that was not searchable or meaningful indexed.

**1. The Emerging Threats Website was Not Searchable or Meaningfully Indexed**

Petitioner fails to raise any argument and present evidence demonstrating that a POSITA or interested member of the public exercising reasonable diligence would have located it. Pet. at 18-19. Petitioner's own evidence indicates that the Emerging Threats rules website was not searchable or meaningfully indexed such that a POSITA exercising reasonable diligence could locate the Emerging Threats file. Goodrich Decl., ¶ 48.

The record evidence demonstrates that the Emerging Threats website lacked a search function (*e.g.*, as a search field or button) that a POSITA might have otherwise used to locate the Emerging Threats reference. Goodrich Decl., ¶ 48. Petitioner's evidence appears to show how the Emerging Threats rules website (*i.e.*, "<http://rules.emergingthreats.net>") currently appears (Ex. 1054) and how it might have appeared in January 12, 2013. Ex. 1030 at 10-11. Both exhibits demonstrate that the rules website had a default Apache homepage, shown below, that contain a filesystem-like directory listing of the website's contents, with columns for "Name," "Last Modified," "Size," and "Description":

There are the Emerging Threats.net Open rulesets.

More information available at <http://www.emergingthreatspro.com> and <http://www.emergingthreats.net>

| <u>Name</u>                 | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|-----------------------------|----------------------|-------------|--------------------|
| <a href="#">blockrules/</a> | 10-Jan-2013 23:30    | -           |                    |
| <a href="#">changelogs/</a> | 11-Jan-2013 19:59    | -           |                    |
| <a href="#">fwrules/</a>    | 11-Nov-2010 10:40    | -           |                    |
| <a href="#">open-nogpl/</a> | 25-Sep-2012 20:54    | -           |                    |
| <a href="#">open/</a>       | 25-Sep-2012 20:54    | -           |                    |
| <a href="#">projects/</a>   | 17-Jan-2011 12:34    | -           |                    |
| <a href="#">research/</a>   | 05-Oct-2012 21:48    | -           |                    |
| <a href="#">version.txt</a> | 11-Jan-2013 19:59    | 5           |                    |

Ex. 1030 at 11; Ex. 1054 (similar).

Nevertheless, the Institution Decision found that, once on the Emerging Threats website, “it would have only required the exercise of reasonable diligence to find the rules list.” DI at 27. The Institution Decision rationalizes that “the number of locations that the rules may be located on the Emerging Threats website is still limited and users would have been able to utilize the ‘Last Modified’ indicator, showing which directories had been modified recently, to narrow down any search, assuming that items that had not been modified for some time would be less worthy of search.” *Id.* However, such an explanation runs contrary to the Federal Circuit’s findings in *Acceleration Bay*.

In *Acceleration Bay*, a technical report was not a printed publication when a “website allowed a user to view a list of technical reports indexed only by author or year.” 908 F.3d at 773. The Board found that the report was not a printed publication, as “an artisan might have located [the reference] by skimming through potentially hundreds of titles in the same year, with most containing unrelated

subject matter, or by viewing all titles in the database listed by author, when the authors were not particularly well known.” *Id.* The Federal Circuit affirmed that the reference was not a printed publication because the reference was not publicly accessible. *Id.*

Like *Acceleration Bay*, the Emerging Threats project provided a website that allowed a user to view a listing of dozens of rule files. Ex. 2016. However, the list is not indexed by author or year. *Id.* Rather, the website is organized into directories with no visible documentation on the directories’ meaning. Goodrich Decl., ¶¶ 50-51. The main page for the Emerging Threats rules website contains links to directories with names like “fwrules” and “blockrules,” which a POSITA would understand to mean “firewall rules” and “block rules” (although it is unclear what the difference is). Goodrich Decl., ¶ 50. Petitioner’s position takes the unreasonable view that a POSITA looking for rules would not traverse directories titles “fwrules” or “blockrules,” but would instead go to subdirectories labelled “open” or “open-nogpl.” Goodrich Decl., ¶ 50; see Ex. 1030 at 11; Ex. 1054. The Emerging Threats rules website’s plain homepage, lacking any useful scheme or labelling, was not meaningfully indexed such that a POSITA might have located the reference even when exercising reasonable diligence. Goodrich Decl., ¶ 51 (citing Ex. 2030 showing an example listing and traversal of the dozens of files in the ET rules websites).

The Board's suggestion about the "Last Modified" column is unsupported by the record evidence.<sup>3</sup> DI at 27. The Last Modified times of directories in Unix-based systems are counterintuitively not affected by content changes to the files in the directory. Goodrich Decl., ¶ 52 (citing Ex. 2013). This is shown in later archival copies of the Emerging Threats website, which shows the open/ and open-nogpl/ directories having unchanged Last Modified. Also inside the directory itself, all the files have the same Last Modified time, rendering the column not as useful in practice. Goodrich Decl., ¶ 52.

## **2. Petitioner's Expert's Testimony is Conclusory and Omits Key Dates and Details**

Conclusory testimony by Petitioner's Expert, Dr. Staniford, fails to demonstrate that the Emerging Threats reference was publicly accessible because the testimony is unsupported and omits key dates and details. Pet. at 19; Ex. 1003

---

<sup>3</sup> Neither the Petition nor the Petitioner's expert declaration assert a theory of public accessibility based on the "Last Modified" column. Patent Owner respectfully submits that "the Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F. 3d 1364, 1381 (Fed. Cir. 2016) (citations omitted).

at ¶¶ 202-206. Dr. Staniford's conclusory statements about the public accessibility of the Emerging Threats reference should be afforded little weight. *See Xerox Corp. v. Bytemark, Inc.*, No. IPR2022-00624, Paper 9 at 15-16 (P.T.A.B. Aug. 24, 2022) (denying institution because the petitioner's expert merely repeated *verbatim* "the conclusory assertion[s] for which it [was] offered to support . . . without any supporting evidence or technical reasoning").

Dr. Staniford alleges that "based on my experience the Emerging Threats rules appear to be true copies of the rules that existed in 2010." Ex. 1003 at ¶ 204. This statement is relevant to the Emerging Threats reference's authenticity (*i.e.* whether the content of the reference is a "true cop[y]"), not its public accessibility. *Id.* This testimony is silent as to any actual dissemination of the Emerging Threats reference, and is silent as to how and whether a skilled artisan could have located the Emerging Threats reference using reasonable diligence, *see* Section V.E.

Dr. Staniford also claims that he "was made aware of the existence of the Bleeding Snort project on multiple occasions, which later became Emerging Threats." Ex. 1003 at ¶ 206. Testimony that the Bleeding Snort project existed does not establish facts relevant to the public accessibility inquiry because it does not establish that a person ordinarily interested in the art would have been aware of the Emerging Threats website generally or the Emerging Threats document specifically. For example, testimony does not establish, that the Emerging Threats document was

(1) “viewed or downloaded,” (2) an “on-line publication was well known to the community interested in the subject matter of the reference,” or (3) that a person interested in the art “would be independently aware of the web address for” the Emerging threats document. *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1349-50 (Fed. Cir. 2016) (citation omitted).

**3. A POSITA Would Not Have Recognized the Relevance of the Emerging Threats Reference Without the Need for Further Research or Experimentation Time**

Even if a skilled artisan was able to locate Emerging Threats and/or the pertinent rule file (a point Patent Owner does not concede), simply being able to locate the reference does not end the inquiry of whether a reference is a printed publication. Rather, persons interested and ordinarily skilled in the art must be able to “recognize and comprehend therefrom the essentials of the claimed invention without need of further research or experimentation.” *Cordis Corp. v. Boston Scientific Corp.*, 561 F.3d 1319, 1333 (Fed. Cir. 2009) (citing *In re Wyer*, 655 F.2d 221, 226 (C.C.P.A. 1981)). Petitioner has failed to show, nor can it show, that a POSITA, would have recognized the relevance of Emerging Threats without the need of further research or experimentation.

Indeed, the Institution Decision acknowledges that “it is not clear that the relevance of Sourcefire and Emerging Threats to the instant Patent would have been immediately apparent once Petitioner learned of the reference.” DI at 12. The

Institution Decision tacitly recognizes that it would have required further research and/or experimentation to review the 11,000+ rules disclosed in Emerging Threats to determine if Emerging Threats was relevant to the '343 Patent. Ex. 1003, ¶ 205.

Further, a keyword search, similar to the one performed in *Lister*, would prove unreasonable. *In re Lister*, 583 F.3d 1307, 1315-16 (Fed. Cir. 2009). In this regard, a keyword search of Emerging Threats for “exfiltration” would have yielded **zero results**. See generally Ex. 1020. Even assuming a keyword search for SSL, TLS, and/or the disclosed HTTP methods was not improper hindsight learned from the '343 Patent as discussed in Section V.B *supra*, such a search would indicate that a skilled artisan would not be able to determine the relevance of Emerging Threats without further research or experimentation. In this regard, searching for SSL and TLS results in 284 rules. *Id.* Searching for HTTP returns over 2800 results. *Id.* Thus, a POSITA, performing a keyword search, would have to review hundreds of rules, similar to the articles in *Acceleration Bay*. Accordingly, a POSITA could not have recognized the relevance of Emerging Threats without further research or experimentation.

Furthermore, the rules in Emerging Threats were not searchable or indexed in a meaningful way that would allow a POSITA to determine the relevance of Emerging Threats without further research or experimentation. Revisiting *Acceleration Bay*, a technical report was not a printed publication when a “website

allowed a user to view a list of technical reports indexed only by author or year.” 908 F.3d at 773. The Board found that the report was not a printed publication because “an artisan might have located [the reference] by skimming through potentially hundreds of titles in the same year, with most containing unrelated subject matter, or by viewing all titles in the database listed by author, when the authors were not particularly well known.” *Id.*

Similar to the facts in *Acceleration Bay*, Emerging Threats provided a website that allowed a user to view a list of thousands of rules indexed only by a Snort ID (SID). Ex. 1020. However, SIDs do not provide a searchable or meaningful index of the rules because SIDs are randomly assigned. Ex. 1004 at 862 (“the system assigns the [new] rule the next available Snort ID number for a local rule and saves the rule in the local rule category.”). Generally, SIDs are classified by their numerical range. For example, rules with a SID less than 100 are reserved for future use, rules with a SID between 100-999,999 are rules that are included with the Snort distribution, and rules with a SID greater than or equal to 1,000,000 are local rules. Ex. 2014 at 141 (Section 3.4.4). Accordingly, SIDs greater than or equal to 1,000,000 are generated by a system when they create a rule. See Ex. 1004 at 862. Indeed, this is supported by Emerging Threat's SID Allocation page, which indicates that rules with a SID between 2,000,000-2,099,999 are allocated to general rulesets, while other ranges of SIDs are allocated to other projects. Ex. 2015 (e.g., “2410000-

2419999 Spyware DNS Rules from the DNS Blackhole”). Thus, the rules cited by Petitioner are local rules generated by a user and a skilled artisan would not be able to locate the rules without first knowing the SID. In its Institution Decision, the Board took similar issue with SIDs. DI at 27. The Board found that persons proceeding to the Emerging Threats website without knowledge of a specific SID “would have found [searching by SID] to be of little help.” *Id.*

At best, a skilled artisan would have to perform additional research and/or experimentation to locate the pertinent rules cited in the Petition by reviewing thousands of unrelated rules contained in Emerging Threats. *See* Ex. 1020; *see also* Ex. 1003 at ¶ 205. However, reviewing thousands of rules far outweighs the reasonable diligence exercised by a POSITA in determining whether a printed publication is potentially relevant. Accordingly, Petitioner has not shown that a POSITA would have recognized the relevance of Emerging Threats without further research or experimentation. Therefore, Emerging Threats is not a printed publication for prior art purposes.

\* \* \*

Petitioner had the burden to prove that the Emerging Threats reference was a printed publication, and they failed to do so. The Board should, therefore, find the Challenged Claims patentable because the instituted ground relies on a reference that is not a prior art printed publication.

## VI. CONCLUSION

For all of these reasons, Patent Owner accordingly requests that the Board confirm the patentability of the Challenged Claims of the '343 Patent.

Respectfully submitted,

Dated: October 30, 2023

/James Hannah/

James Hannah (Reg. No. 56,369)  
Jenna Fuller (Reg. No. 74,212)  
KRAMER LEVIN NAFTALIS & FRANKEL LLP  
Twin Dolphin Drive, Suite 700  
Redwood Shores, CA 94065  
Tel: 650.752.1700 Fax: 650.752.1800  
jhannah@kramerlevin.com  
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  
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  
skelly@bannerwitcoff.com  
bwright@bannerwitcoff.com  
jhutchins@bannerwitcoff.com

(Case No. IPR2023-00446)

*Attorneys for Patent Owner*  
Centripetal Networks, LLC

**CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24**

The undersigned hereby certifies that the foregoing PATENT OWNER'S RESPONSE has 10,138 words in compliance with the 14,000 word limit set forth in 37 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 30, 2023

/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  
jhannah@kramerlevin.com  
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  
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  
skelly@bannerwitcoff.com  
bwright@bannerwitcoff.com  
jhutchins@bannerwitcoff.com

(Case No. IPR2023-00446)

*Attorneys for Patent Owner*  
Centripetal Networks, LLC

**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 30, 2023                                                                                                                                                                                                                                          |
| <i>Manner of service</i> | Electronic Filing with the Board                                                                                                                                                                                                                          |
| <i>Documents served</i>  | PATENT OWNER'S RESPONSE                                                                                                                                                                                                                                   |
| <i>Persons Served</i>    | REED SMITH LLP<br>Gerard M. Donovan<br>Peter J. Chassman<br>Walter M. Egbert<br>Jonathan I. Detrixhe<br>Sidharth Kapoor<br>gdonovan@reedsmith.com<br>pchassman@reedsmith.com<br>wegbert@reedsmith.com<br>jdetrixhe@reedsmith.com<br>skapoor@reedsmith.com |

By: /James Hannah/  
James Hannah (Reg. No. 56,369)