

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2023-00446

U.S. Patent 10,567,343 B2

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	Page
I. Introduction	1
II. Claim Construction	1
III. Sourcefire In View of Emerging Threats Renders Claims 1-20 Obvious.....	3
A. Emerging Threats Teaches “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.....	5
1. Rule 2003021 Prevents An Exfiltration Operation.....	5
2. Many Emerging Threats Rules Teach Matching Application Header Field Values To Prevent Exfiltration Operations.....	8
3. Emerging Threats Rules Apply Packet Transformation Functions “Responsive to” A Determination Based on Application Packet Header	9
B. The Obviousness Analysis Is Grounded in the Teachings of Sourcefire And Emerging Threats	10
C. Sourcefire and Emerging Threats Render Obvious Claims 5 and 12	13
D. PO’s Secondary Consideration Arguments Lack Merit And A Nexus To The Claims	13
1. The ‘343 Alleged Invention Does Not Addresses Any Long-Felt But Unresolved Need.....	14
2. The ‘343 Alleged Invention Was Not The Subject of Industry Praise	16
E. Emerging Threats Is A Printed Publication.....	17
1. The Emerging Threats Website Made The Rules Available To Persons Exercising Reasonable Diligence.....	21
2. Dr. Staniford’s Testimony Is Grounded in Facts	23
3. A POSITA Would Have Recognized The Relevance of Emerging Threats	25
IV. Conclusion.....	27

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Acceleration Bay, LLC v. Activision Blizzard, Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	21, 27
<i>Apple, Inc. v. Ameranth, Inc.</i> , CBM2015-00080, Paper 44 (Aug. 26, 2016)	14
<i>Blue Calypso, LLC v. Groupon, Inc.</i> , 815 F.3d 1331 (Fed. Cir. 2016)	22
<i>Cisco Systems, Inc. v. Centripetal Networks, Inc.</i> , IPR2018-01760, Paper 41 (May 18, 2020).....	16
<i>Cordis Corp. v. Boston Scientific Corp.</i> , 561 F.3d 1319 (Fed. Cir. 2009)	26
<i>In re Etter</i> , 756 F.2d 852 (Fed. Cir. 1985)	4
<i>Fox Factory, Inc. v. SRAM, LLC</i> , 944 F.3d 1366 (Fed. Cir. 2019).....	14, 15
<i>In re Lister</i> , 583 F.3d 1307 (Fed. Cir. 2009)	26
<i>MBO Labs., Inc. v. Becton, Dickinson & Co.</i> , 474 F.3d 1323 (Fed. Cir. 2007)	3
<i>In re Mouttet</i> , 686 F.3d 1322 (Fed. Cir. 2012)	4
<i>Mylan Pharmaceuticals Inc. et al v. Sanofi-Aventis Deutschland GmbH</i> , IPR2019-00122, Paper 83 (May 29, 2022).....	16
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	2

<i>Novartis AG v. Torrent Pharms. Ltd.</i> , 853 F.3d 1316 (Fed. Cir. 2017)	14
<i>Samsung Elecs. Co. v. Infobridge Pte. Ltd.</i> , 929 F.3d 1363 (Fed. Cir. 2019)	23
<i>Ex parte Thompson</i> , Appeal No. 2011-011620 (P.T.A.B. Mar. 21, 2014) (designated as informative on Apr. 14, 2020)	14
<i>Voter Verified, Inc. v. Premier Election Solutions, Inc.</i> , 698 F.3d 1374 (Fed. Cir. 2012)	22, 23, 24

PETITIONER'S UPDATED EXHIBIT LIST

Exhibit No.	Title
EX-1001	U.S. Patent No. 10,567,343 ("the '343 Patent")
EX-1002	File History of the '343 Patent ("File History")
EX-1003	Declaration of Dr. Stuart Staniford in support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 10,567,343
EX-1004	Sourcefire 3D System User Guide Version 4.10 ("Sourcefire"), available at https://www.scribd.com/document/96860221/Sourcefire-3D-System-User-Guide-v4-10
EX-1005	IPR2018-01760 CS-1005: Declaration of John Leone
EX-1006	Bard, G.V., "Cryptology ePrint Archive: Report 2006/136: A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL," archived at Internet Archive Wayback Machine on May 3, 2006 at https://web.archive.org/web/20060503043443/http://eprint.iacr.org:80/2006/136
EX-1007	Barry M. Leiner et al., "A Brief History of the Internet," Internet Society, 1997, available at: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
EX-1008	U.S. Pat. No. 7,032,031 ("Jungck")
EX-1009	E. H. Spafford, "The Internet Worm Program: An Analysis," <i>Purdue Technical Report CSD-TR-823</i> , 1988, available at: https://spaf.cerias.purdue.edu/tech-reps/823.pdf

Exhibit No.	Title
EX-1010	Eichin, M.W. and Rochlis, J.A., "With Microscope and Tweezers: The Worm from MIT's Perspective," <i>Communications of the ACM</i> , Volume 32 Number 6, June 1989; <i>available at</i> https://www.cs.jhu.edu/~fabian/courses/CS600.624/Rochlis_morris.pdf
EX-1011	T. Eisenberg <i>et al.</i> , "The Cornell Commission: On Morris and the Worm," <i>Communications of the ACM</i> , Volume 32 Number 6, June 1989; <i>available at</i> https://www.cs.cornell.edu/courses/cs1110/2009sp/assignments/a1/p706-eisenberg.pdf
EX-1012	J. C. Mogul, "Simple and Flexible Datagram Access Controls for Unix-based Gateways," Digital Western Research Laboratory Technical Report No. 89/4, 1989; <i>available at</i> https://www.hpl.hp.com/techreports/Compaq-DEC/WRL-89-4.pdf
EX-1013	Declaration of John M. Hendricks In Support IPR Petition for U.S. Pat. 10,567,343 (<i>served as supplemental evidence in response to objections, but not filed</i>)
EX-1014	Affidavit of Christopher Butler, dated Jan. 11, 2023, authenticating EX-1038, EX-1073, EX-1080 (<i>served as supplemental evidence in response to objections, but not filed</i>)
EX-1015	Affidavit of Christopher Butler, dated Jan. 12, 2023, authenticating Emerging Threats (EX-1020) (<i>served as supplemental evidence in response to objections, but not filed</i>)
EX-1016	Heberlein, L. T.L, <i>et al.</i> , "A Network Security Monitor," <i>Proceedings, 1990 IEEE Computer Society Symposium on Security and Privacy</i> , 1990, <i>available at</i> https://ieeexplore.ieee.org/document/63859 .

Exhibit No.	Title
EX-1017	IPR2018-01760 CS-1017: "NetRanger Network Security Management System User Guide". v1.3.1 <i>Wheelgroup Corporation</i> , 1997.
EX-1018	Roesch, M., "Snort: Lightweight Intrusion Detection for Networks," <i>Lisa</i> (Vol. 99, No. 1, pp. 229-238), 1999, <i>available</i> at https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf
EX-1019	U.S. Pat. No. 8,370,936 ("Zuk")
EX-1020	Emerging Threats, available at https://web.archive.org/web/20101202025325/http://rules.emergingthreats.net/open/snort-2.8.4/emerging-all.rules (Dec. 2, 2010).
EX-1021	Authorized Classification and Control Markings Register, Vol. 1, Ed. 2 (Version 1.2), May 12, 2008, available at http://sgp.fas.org/othergov/intel/register.pdf
EX-1022	"Transmission Control Protocol," <i>IETF RFC 793</i> . J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 2, 2007 at https://web.archive.org/web/20070202201546/https://tools.ietf.org/html/rfc793 .
EX-1023	"Internet Protocol," <i>IETF RFC 791</i> , J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 4, 2007 at https://web.archive.org/web/20070204151303/http://tools.ietf.org/html/rfc791 .
EX-1024	"File Transfer Protocol," <i>IETF RFC 765</i> , J. Postel, ed., June 1980, archived at Internet Archive Wayback Machine on February 6, 2007 at

Exhibit No.	Title
	https://web.archive.org/web/20070206005843/https://tools.ietf.org/html/rfc765 .
EX-1025	T. B. Lee, "The Original HTTP as defined in 1991," World Wide Web Consortium, 1991, archived at Internet Archive Wayback Machine on June 5, 1997 at https://web.archive.org/web/19970605071155/https://www.w3.org/Protocols/HTTP/AsImplemented.html .
EX-1026	I. Ristic, "SSL/TLS and PKI History," April 2018, available at https://www.feistyduck.com/ssl-tls-and-pki-history/ .
EX-1027	Service Name and Transport Protocol Port Number Registry, Internet Assigned Numbers Authority (IANA), available at https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
EX-1028	Understanding /etc/passwd File Format, available at https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/
EX-1029	ASCII Table, available at https://www.asciitable.com/
EX-1030	Affidavit of Nathaniel E Frank-White, Internet Archive, Archive.org (Dec. 12, 2022)
EX-1031	<i>Intentionally Left Blank</i>
EX-1032	K. Ingham & S. Forrest, "A History and Survey of Network Firewalls," <i>University of New Mexico Computer Science Department Technical Report 2002-37</i> , 2002, available at https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf .
EX-1033	Sourcefire Support Website Webpage, archived at Internet Archive Wayback Machine on April 30, 2011, available at

Exhibit No.	Title
	https://web.archive.org/web/20110430194135/https://support.sourceforge.com/ (“Sourcefire Support Webpage”).
EX-1034	Crow, J., Bennet, B.; Structure of Social Security Numbers, available at https://www.eff.org/pages/structure-social-security-numbers
EX-1035	<i>Curriculum Vitae</i> of Stuart Staniford
EX-1036	Webster's New World Computer Dictionary, Tenth Edition (2003)
EX-1037	Microsoft Computer Dictionary, Fifth Edition (2002)
EX-1038	T. Dierks & E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1,” IETF RFC 4346, April 2006, archived at Internet Archive Wayback Machine on June 26, 2006 at https://web.archive.org/web/20060626134135if_/http://www.ietf.org:80/rfc/rfc4346.txt
EX-1039	<i>Intentionally Left Blank</i>
EX-1040	Minoli, Daniel, et al., Minoli-Cordovana's Authoritative Computer & Network Security Dictionary (2006)
EX-1041	Dictionary Of Computing & Communications, McGraw-Hill (2003)
EX-1042	IPR2018-01436 CS-1003: Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of US Patent No. 9,124,552.
EX-1043	U.S. Patent No. 9,124,552

Exhibit No.	Title
EX-1044	IPR2018-01437 CS-1003: Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of US Patent No. 9,160,713
EX-1045	IPR2018-01760 CS-1038, Declaration of Christopher Butler
EX-1046	IPR2018-01760 CS-1042, Declaration of Jacob H. Baugher III
EX-1047	U.S. Patent No. 8,356,357
EX-1048	U.S. Patent No. 8,141,127
EX-1049	Declaration of John M. Hendricks In Support IPR Petition for U.S. Pat. 10,193,917
EX-1050	M. Edwards, "Bleeding Edge of Snort," Oct. 10, 2004, available at https://www.itprotoday.com/windows-78/bleeding-edge-snort
EX-1051	The Aggregation Point for Snort Signatures and Research, Bleedingsnort.com, Wayback Machine, Internet Archive, available at https://web.archive.org/web/20041230024004/http://www.bleedingsnort.com/
EX-1052	<i>Intentionally Left Blank</i>
EX-1053	Emerging Threats Rule Documentation Wiki, available at https://doc.emergingthreats.net/
EX-1054	Proofpoint Emerging Threats Rules, available at https://rules.emergingthreats.net/
EX-1055	<i>Intentionally Left Blank</i>

Exhibit No.	Title
EX-1056	<i>Intentionally Left Blank</i>
EX-1057	<i>Intentionally Left Blank</i>
EX-1058	U.S. Patent No. 9,160,713
EX-1059	<i>Intentionally Left Blank</i>
EX-1060	<i>Intentionally Left Blank</i>
EX-1061	<i>Intentionally Left Blank</i>
EX-1062	IPR2018-01559 CS-1003: Declaration of Dr. Stuart Staniford in Support of Petition for Inter Partes Review of US Patent No. 9,686,193
EX-1063	U.S. Patent No. 9,686,193
EX-1064	<i>Intentionally Left Blank</i>
EX-1065	<i>Intentionally Left Blank</i>
EX-1066	<i>Intentionally Left Blank</i>
EX-1067	Cisco Systems, Inc., v. Centripetal Networks, Inc., IPR2018-01436 at Paper 40 (Final Written Decision) (U.S. Pat. 9,124,552)
EX-1068	Cisco Systems, Inc., v. Centripetal Networks, Inc., IPR2018-01437 at Paper 40 (Final Written Decision) (U.S. Pat. 9,160,713)
EX-1069	Centripetal Networks, Inc. v. Cisco Sys., 2020-1635 (Fed. Cir. Mar. 10, 2021), available via https://cafc.uscourts.gov/opinions-orders/20-1635.opinion.3-

Exhibit No.	Title
	10-2021_1745854.pdf (decision on appeal from '552 and '713 FWDs)
EX-1070	Cisco Systems, Inc., v. Centripetal Networks, Inc., IPR2018-01559 at Paper 7 (Decision Denying Institution of Inter Partes Review) (U.S. Pat. 9,686,193)
EX-1071	<i>Intentionally Left Blank</i>
EX-1072	<i>Intentionally Left Blank</i>
EX-1073	“Hypertext Transfer Protocol -- HTTP/1.1” IETF RFC 2616. R. Fielding, et al., June 1999, archived at Internet Archive Wayback Machine on January 9, 2005 at https://web.archive.org/web/20050119021312/https://www.ietf.org/rfc/rfc2616.txt .
EX-1074	HTTP-Requests, available at https://www.tutorialspoint.com/http/http_requests.htm
EX-1075	HTTP – Responses, available at https://www.tutorialspoint.com/http/http_responses.htm
EX-1076	IPR2021-01155 CS-1003: Declaration of Dr. Robert Akl in Support of Petition for Inter Partes Review of US Patent No. 10,567,343
EX-1077	Palo Alto Networks, Inc., v. Centripetal Networks, Inc., IPR2021-01155 at Paper 12 (Decision Denying Institution of Inter Partes Review) (U.S. Pat. 10,567,343)
EX-1078	Emerging Threats FAQ, available at https://doc.emergingthreats.net/bin/view/Main/EmergingFAQ
EX-1079	<i>Intentionally Left Blank</i>

Exhibit No.	Title
EX-1080	Snort rules 2.4 ftp.rules, available via https://web.archive.org/web/20060112054053/http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz
EX-1081	Declaration of Dr. Sean Moore in Support of Centripetal's Responses to Non-Final Office Action in Re-examination of '193 patent.
EX-1082	Centripetal Networks Press Release, "Centripetal Networks Inc. Adds Emerging Threats IQRisk® Rep List and IQRisk Query for Their RuleGate® Appliance". Downloaded from https://www.centripetal.ai/press-releases/centripetal-emerging-threats-rulegate/
EX-1083	Cisco Systems, Inc., v. Centripetal Networks, Inc., IPR2018-01559, Patent Owner's Preliminary Response. (U.S. Pat. 9,686,193).
EX-1084	Palo Alto Networks, Inc., v. Centripetal Networks, Inc., IPR2021-01155, Patent Owner's Preliminary Response. (U.S. Pat. 10,567,343).
EX-1085	Ex-Parte Re-examination History for Patent 9,686,193.
EX-1086	Palo Alto Networks, Inc., v. Centripetal Networks, Inc., IPR2021-01155, Paper 16: Decision Denying Petitioner's Request for Rehearing.
EX-1087	Cisco Systems, Inc., v. Centripetal Networks, Inc., IPR2018-01436, Patent Owner's Preliminary Response. (U.S. Pat. 9,124,552).
EX-1088	Gartner, August 2011. Magic Quadrant for Content-Aware Data Loss Prevention. Obtained by SS from

Exhibit No.	Title
	https://www.etruserve.com.tw/gtb/GTB%20wp/rp-gartner-magic-quadrant-dlp-2011.pdf
EX-1089	US Patent No. 8,565,108.
EX-1090	US Patent No. 7,467,202.
EX-1091	<i>Intentionally Left Blank</i>
EX-1092	<i>Intentionally Left Blank</i>
EX-1093	<i>Intentionally Left Blank</i>
EX-1094	S. Turner & C. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0," IETF RFC 6176, March 2011, archived at Internet Archive Wayback Machine on March 18, 2011 at https://web.archive.org/web/20110318184421/https://tools.ietf.org/html/rfc6176 .
EX-1095	M. Chatel, "Classical vs. Transparent IP Proxies," <i>IETF RFC 1919</i> , March 1996, available at https://web.archive.org/web/20070630145311/https://tools.ietf.org/html/rfc1919
EX-1096	E. Rescorla, "HTTP over TLS", <i>IETF RFC 2818</i> , May 2000, archived at Internet Archive Wayback Machine on January 25, 2007 at https://web.archive.org/web/20070125003236/https://tools.ietf.org/html/rfc2818 .
EX-1097	J. Moser, "The First Few Milliseconds of an HTTPS Connection", <i>Moserware</i> , June 10, 2009, archived at Internet Archive Wayback Machine on June 13, 2009 at https://web.archive.org/web/20090613041022/http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html

Exhibit No.	Title
EX-1098	Apple Quicktime RTSP URL buffer overflow. IBM advisory for CVE-2007-0015, 2007, available at https://exchange.xforce.ibmcloud.com/vulnerabilities/31203
EX-1099	Real Time Streaming Protocol (RTSP). RFC 2326, April 1998. Available at https://www.rfc-editor.org/rfc/rfc2326.html
EX-1100	Deposition Transcript of Dr. Goodrich (Jan. 5, 2024)
EX-1101	Deposition Transcript of Mr. Pedro Marinho (Jan. 23, 2024)
EX-1102	Emerging Threats archived webpage, available at https://web.archive.org/web/20101123160511/http://www.emergingthreats.net/

I. Introduction

The Petition showed that Emerging Threats qualifies as prior art and that Sourcefire and Emerging Threats render the claims obvious. Patent Owner (“PO”) argues in its Response (“POR”) that the “prevent an exfiltration operation” element was not taught. However, testimony from PO’s expert and its own employee, Mr. Marinho, supports the Petition and shows that Emerging Threats teaches rules configured to be triggered by exfiltration operations. PO’s secondary considerations arguments lack a nexus to the ’343 claims, and Mr. Marinho’s testimony that he learned of, downloaded, and used Emerging Threats prior to 2010 rebuts PO’s arguments about Emerging Threats qualifying as prior art.

For the reasons in the Petition, the Institution Decision, and below, Sourcefire and Emerging Threats render the challenged claims obvious.

II. Claim Construction

Claim element 1[e]¹ requires “... applying ... at least one packet transformation function *configured to prevent an exfiltration operation.*” EX-1001 11:54-58 (emphasis added). PO seeks no construction, but notes that it argued for the plain meaning of this term in litigation. POR 18.

¹ Independent claims 8 and 15 include counterpart elements.

However, PO argues that the claims prevent exfiltrations “while still preserving the flow of normal legitimate network traffic without disruption.” POR 10, *citing* EX-1001 7:35-40. PO also argues that rules are not configured to prevent exfiltration where PO avers that the rule is overbroad (also blocking legitimate traffic) or too specific (also allowing some exfiltrations). *E.g.*, POR 11, 18 (arguing Rule 2003021 does not prevent exfiltration because it can be defeated by sending data over a different port). Thus, it appears the parties dispute whether “configured to prevent an exfiltration operation” has its plain meaning or requires preventing exfiltrations while not having some amount of false positives or negatives, as PO implicitly asserts. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (construction is only required when necessary to resolve a controversy).

The Board should reject PO's attempt to read additional vague requirements into the term because the claim language is clear: “configured to prevent an exfiltration operation.” It does not require preventing all exfiltrations or allowing all non-exfiltration traffic.

Further, the '343 specification contradicts PO's tacit construction. It discloses only two methods—HTTP and HTTPS methods—“to prevent exfiltrations.” EX-1001 8:59-62.

The HTTP method allows packets with a GET application header field value and blocks HTTP packets with POST, PUT, DELETE, or CONNECT, because “attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data.” *Id.* 7:4-27; 7:51-8:6. The HTTP method blocks exfiltrations using POST methods, but also legitimate packets using POST methods.

The HTTPS method allows packets with TLS 1.1 or 1.2 application header field values and blocks packets with TLS 1.0, “because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions.” *Id.* 6:61-7:3; 8:7-38. The HTTPS method thus blocks exfiltrations as well as legitimate packets using TLS 1.0. The HTTP and HTTPS methods do not block exfiltrations mediated by other methods.

Given this disclosure, construing “prevent an exfiltration operation” to require a rule to somehow satisfy breadth or narrowness requirements would improperly exclude these embodiments. *MBO Labs., Inc. v. Becton, Dickinson & Co.*, 474 F.3d 1323, 1333 (Fed. Cir. 2007) (a construction that excludes preferred embodiments is “rarely, if ever, correct.”).

III. Sourcefire In View of Emerging Threats Renders Claims 1-20 Obvious

PO argues that a POSITA would not implement commented-out rules in Emerging Threats. POR 12. However, a Sourcefire user would import rules and tune them to the network environment, including selectively activating and setting

rules to block or alert. Pet. 81; EX-1003 ¶¶268-269. Dr. Staniford further explained that uncommenting rules that were commented-out would enable them. Ex. 2011 67:10-68:24, 69:8-72. Emerging Threats' instructions to enable rules where useful further shows it was well-known to enable rules. EX-1020 109 (SID:2001328) ("Enable it where useful"). PO's declarants confirmed that commented-out rules could be enabled. EX-1100 27:16-21; EX-1101 71:3-11, 75:10-23.

More fundamentally, Emerging Threats teaches rules configured to be triggered by exfiltration operations even if some of them were disabled because they may not be used in all environments. As Dr. Staniford testified, they show that a POSITA knew of rules triggered by exfiltration operations independent of whether they were enabled. Ex. 2011 72:5-11. Emerging Threats' teachings of rules configured to detect exfiltration operations (even if disabled) in combination of Sourcefire's teaching of loading and enabling rules to inspect and block or allow packets render the claims obvious. *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements."); *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc) (whether one reference can be incorporated in another is "basically irrelevant" since the test for obviousness is "not whether the references could be physically combined but

whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole”).

A. Emerging Threats Teaches “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

1. Rule 2003021 Prevents An Exfiltration Operation

The Petition identified Rule 2003021 as configured to detect an exfiltration operation transmitting traffic to unusual ports using an out-of-date encryption protocol, and Sourcefire teaches enabling rules and using them to block traffic. Pet. 57. The rule identifies exfiltrations by checking an application header field value for traffic using an out-of-date encryption version. Pet. 57-58.

PO's employee, Mr. Marinho, confirmed that malware exfiltrating data would trigger this rule, but noted that other packets could trigger it too if they included the same content match in the first bits of the application header. EX-1101 77:16-78:11. Dr. Goodrich also acknowledged that exfiltration using SSLv3 on a high port would trigger the rule. EX-1100 62:18-25. Thus, Rule 2003021 triggers when an application header field value includes content indicating an out-of-date SSL/TLS version—exactly how the '343 patent's HTTPS method prevents exfiltrations.

The record undermines PO's assertion that Rule 2003021 is instead a signature designed to identify good SSL/TLS sessions at high ports. POR 16, citing Ex. 2010 ¶78, Ex. 2018, Ex. 2019. Ex. 2018 indicates the impetus to create the rule

was “a new attack, a malicious bot, if you will, that is using standard SSL ... it’s a command and control bot that then is a risk to any computer that has the bot infecting it.” EX-1100 36:15-37:5; 39:12-40:19; Ex. 2018. The rule detects outbound traffic (“\$HOME_NET any -> \$EXTERNAL_NET 124:65535”) from such a computer using an outdated, insecure encryption protocol. EX-1003 ¶¶263-265, 267. Dr. Goodrich admitted that a command-and-control attack gives an attacker control of a compromised computer, but could not answer whether command-and-control sessions are used for exfiltration. *Id.* 37:19-38:11. Mr. Marinho, however, confirmed that a reason malware would communicate with a command-and-control server is to exfiltrate data. EX-1101 116:24-118:9 (testifying in context of a rule that prevents exfiltration based on HTTP POST methods). Dr. Staniford also explained that it was common for malware to exfiltrate data to a command-and-control server. Ex. 2011 139:12-22 (typical trojan action is to take form data, which often contains log-in credentials, and upload it to the malware command-and-control center).

PO also argues that Rule 2003021 should be read with others in the ruleset that prevent alerts for SSL traffic, regardless of version, on specific ports. POR 17. Those other rules identify good SSL/TLS sessions on high ports, and Rule 2003021 uses those additional rules to reduce false positives in its exfiltration detections. EX-1100 42:2-49:16 (Dr. Goodrich explaining that Rules 2003026 (EX-1020 107)

through 2008543 cause the system to not alert for SSL traffic on known ports). Rule 2003021 would therefore not be triggered by exfiltrations on those ports. *Id.* 61:16-62:25. Thus, reading the rule in conjunction with those before it in the ruleset shows that Emerging Threats teaches preventing exfiltrations while preserving the flow of legitimate network traffic on known ports.

PO's assertion that no evidence shows "correlation between high ports and exfiltration operations" (POR 18) is wrong. Dr. Staniford explained the correlation. Ex. 2011 102:24-103:21. PO also misses the point. A POSITA would have understood that the rule was configured to identify exfiltration of encrypted data via the use of a vulnerable SSL/TLS version. Pet. 54; EX-1003 ¶267. The rule checks application header field values to identify traffic using a vulnerable encryption protocol, which indicates that the rule detects exfiltrations. Ex. 2011 102:5-23.

PO also challenges Dr. Staniford's prior work relating to exfiltration detection and prevention because one implementation involved large, encrypted transmissions. POR 18, *citing* Ex. 2011 93:8, 94:2-6. However, that experience provided context for understanding the traffic that the rule was configured to capture by detecting SSLv3 traffic on unusual ports. Ex. 2011 96:11-97:3. Thus, Dr. Staniford's experience positions him well to opine about what a POSITA would have understood reading the rule in 2010. *Id.* 62:12-63:7 (by 2006 Dr. Staniford "knew very well there were exfiltration Snort rules").

2. Many Emerging Threats Rules Teach Matching Application Header Field Values To Prevent Exfiltration Operations

PO mistakenly asserts that other Emerging Threats rules do not match application header field values. POR 19-21. Emerging Threats contains numerous rules targeting exfiltration operations in this way. Pet. 56.

For example, Rule 2005319 detects traffic with application header field values containing POST—just like the '343 patent's HTTP-EXFIL method. Pet. 61-62; EX-1020 45; EX-1003 ¶277. This rule also preserves the flow of legitimate traffic by checking for a URI portion associated with spyware (uricontent:“/zuzu.php?&r=”), thus satisfying PO's tacit construction. *Id.*

Communications with a command-and-control server would trigger this rule, including exfiltrations. Ex. 2011 84:22-87:88. As Dr. Staniford explained, the “spyware” comment “certainly suggests that this software is capable of exfiltrating data.” *Id.* Mr. Marinho confirmed that this rule checks whether outbound packets contain a POST application header field value. EX-1101 104:22-105:3, 106:2-9. He also identified the rule as designed to detect spyware and explained that “spywares were designed to actually spy, to collect information on the system and exfiltrate it.” EX-1101 109:5-110:13.

Rule 2010234 likewise teaches detecting a POST application header field value as taught by the '343 patent. Pet. 64-65; EX-1020 18; EX-1003 ¶¶282-284. This rule is again like the '343 patent's HTTP-EXFIL method, except targeted to

also check URI content to have less false positives to preserve the flow of legitimate traffic. Ex. 2011 80:19-82:16. Mr. Marinho agreed that the rule alerts on packets leaving a network with specific application header field values (EX-1101 110:14-21, 115:6-18) and admitted that it is designed to detect traffic to a command-and-control server, and a reason for which is data exfiltration. EX-1101 115:19-116:16, 117:25-119:9.

Rule 2006409 further exemplifies detecting a POST application header field value, like the HTTP-EXFIL method. EX-1020 98; EX-1003 ¶159; Ex. 2011 79:11-80:15.

Rule 2003937 is yet another example. Ex. 2011 63:18-65:21; EX-1020 155. The comments indicate that the rule detects a “trojan leaking user data”—unquestionably exfiltration. *Id.* It does so by detecting a POST application header field value and additional content in a post going to a remote web server. *Id.*

These examples show that Emerging Threats teaches many rules configured to be triggered by exfiltration operations, rebut PO's assertion that other exfiltration rules do not match application header field values, and rebut PO's argument that the rules identified in the Petition fail to preserve the flow of network traffic.

3. Emerging Threats Rules Apply Packet Transformation Functions “Responsive to” A Determination Based on Application Header Field Values

PO's assertion that no Emerging Threats rules 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 operator's second criterion (POR 21-23) is misguided because it attacks the teachings of Emerging Threats alone while the Petition shows the combined teachings of Sourcefire and Emerging Threats render the element obvious. Pet. 56-58. PO also ignores specific Emerging Threats rules teaching applying a packet transformation function responsive to a determination based on an application header field value. For example, Rule 2003021 triggers responsive to determining that a packet includes an SSLv3 application header field value. Pet. 56-57; *see supra* § III.A.1. Rules 2005319 and 2010234 trigger upon determining that a packet includes an HTTP POST method application header field value. Pet. 61-62, 64-65; *see supra* § III.A.2. Sourcefire teaches that rules may be loaded and set to alert or drop. Pet. 56-57. Thus, Sourcefire in view of Emerging Threats teaches the claim.

B. The Obviousness Analysis Is Grounded in the Teachings of Sourcefire And Emerging Threats

PO asserts that Petitioner relies on impermissible hindsight. POR 23. While PO asserts that the inventor devised preventing exfiltrations without hampering the web, the '343 patent discloses two methods for preventing exfiltrations—one that blocks traffic using HTTP methods other than GET and another that blocks traffic using an out-of-date encryption protocol. *See* § II above. Long before the purported

invention, Emerging Threats disclosed rules that were likewise configured to identify exfiltration operations by detecting packets with application header field values indicating the use of an out-of-date encryption protocol (SID:2003021 discussed *supra* § III.A.1) and HTTP POST methods (SID:2005319 and SID:2010234 discussed *supra* § III.A.2). Sourcefire teaches loading and using rules like these to selectively block or allow traffic. Pet. 56-57; EX-1003 ¶¶162-163. Thus, the claimed invention was taught by the prior art—no hindsight needed.

PO's argument that it was nonobvious to implement these rules to prevent exfiltrations (POR 23) is unfounded. As the rules' comments indicate, and Mr. Marinho confirmed, these rules are designed to be triggered by outbound traffic associated with malware that could be used for exfiltration. *See supra* § III.A.1 & III.A.2. Dr. Staniford explains the obvious desirability of blocking such traffic. EX-1003 ¶¶208 (a rule would be set to block traffic when aligned with network security goals, such as to block exfiltration), 284 (it is desirable to block activities of malware).

Further, Dr. Staniford had extensive experience with such rules long before the 2013 priority claim. EX-1003 ¶¶15-18; Ex. 2011 14:17-23 (working with Snort from the late '90s), 17:2-18:20 (work with Snort in early 2000s). He taught Snort rules to Cornell students by 2013. Ex. 2011 77:1-16. He had specific experience with rules for exfiltrations before 2010. Ex. 2011 23:23-24:10 (working with Snort

at FireEye 2005-2006), 26:14-27. Dr. Staniford recognized Rule 2003021 as targeting exfiltration since it uses an out-of-date version of SSL on a high numbered port, and he was “using essentially this for exfiltration detection at FireEye.” Ex. 2011 102:5-23, 113:13-116:6. In addition, security vulnerabilities with SSL 3.0 and TLS 1.0 were well-known. EX-1003 ¶128, EX-1006 1, EX-1038 1 (TLS 1.1 release in 2008). Dr. Staniford also explained that it was known in the ‘90s that POST methods were used for exfiltrations. Ex. 2011 65:15-21, 99:9-101:10. Dr. Staniford grounds his opinions in his experience, not hindsight.

In contrast, PO relies on declarants lacking relevant expertise prior to the ‘343 patent. Dr. Goodrich had no specific experience with Snort rules prior to his retention by PO sometime after 2016. EX-1100 13:18-15:2. Mr. Marinho had experience in the context of managing Intrusion Detection Systems, not Intrusion Prevention Systems (which can drop traffic). EX-1101 28:19-29:15. Given their lack of experience, the Board should discount their assertions that POSITAs in 2010 would not have blocked traffic using rules targeting exfiltrations.

PO’s 2014 press release touting Emerging Threats as the world-leading provider of threat intelligence rulesets also does not demonstrate hindsight; it explains that the project had been around for over a decade and grown to be the “de facto standard in network-based malware threat detection” by that time. POR 35;

EX-1082. Mr. Marinho confirmed that Emerging Threats was known to the interested public years earlier. EX-1101 14:15-20:23.

C. Sourcefire and Emerging Threats Render Obvious Claims 5 and 12

Claims 5 and 12 recite “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.” PO wrongly asserts that the Petition fails to identify analysis of application header field values for these claims. POR 26. SID:2010234 checks application header field values for POST methods and specific URI content. Pet. 64. Mr. Marinho confirmed that packets with application header field values POST and URI content trigger the rule. EX-1101 115:13-18.

PO's argument that modifying the rule to drop traffic shows hindsight also fails. POR 26. Sourcefire teaches setting rules to allow or drop traffic, and as discussed above it was desirable to block detected outbound traffic to a command-and-control server. *See supra* §§ III.A.2 & III.B.

D. PO's Secondary Consideration Arguments Lack Merit And A Nexus To The Claims

PO's secondary considerations arguments lack a nexus to the claims and fail to overcome the strong showing of obviousness.

1. The '343 Alleged Invention Does Not Address Any Long-Felt But Unresolved Need

PO has not established that the '343 patent or its products that they allege embody the patent fulfilled a long-felt need or that others failed in fulfilling that need. To establish a long-felt need, (1) the need must have been a persistent one that was recognized by ordinarily skilled artisans; (2) the need must not have been satisfied another before Applicant's invention; and (3) the invention must, in fact, satisfy the need. *Ex parte Thompson*, Appeal No. 2011-011620 (P.T.A.B. Mar. 21, 2014) (designated as informative on Apr. 14, 2020). PO must also establish "a nexus between the merits of the claimed invention and the evidence of secondary considerations" for the evidence to be given substantial weight. *Apple, Inc. v. Ameranth, Inc.*, CBM2015-00080, Paper 44 at 36–37 (Aug. 26, 2016).

There is no long-felt need because, as the Petition showed, the alleged need solved by the '343 claims was solved years earlier by Sourcefire and Emerging Threats. Pet. 27-67; *supra* § III. *Novartis AG v. Torrent Pharms. Ltd.*, 853 F.3d 1316, 1331 (Fed. Cir. 2017) ("In evaluating whether the requisite nexus exists, the identified objective indicia must be directed to what was *not* known in the prior art.").

Even if it was not already well-known to implement Snort rules to prevent an exfiltration operation, PO has also not shown there to be any long-felt need for the claims of the '343 patent. *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373

(Fed. Circ. 2019) (“To determine whether the patentee has met that burden, we consider the correspondence between the objective evidence and the claim scope.”). PO’s assertion that its products fulfilled a long-felt need lacks a nexus to the claims. POR 28–32. PO does not present any evidence that could show that these products embody the claims. Instead, PO relies upon its expert’s assertions of the need and that it was satisfied by the ’343 patent and PO’s products. POR 27-32; *citing* Ex. 2010 ¶¶104-112. Rather than basing his opinions on his own analysis, however, Dr. Goodrich relies on a conclusory declaration from PO’s Chief Technology Officer and the named inventor on the patent, Dr. Sean Moore. Ex. 2010 ¶¶104-112, *citing* EX-1081 ¶¶5-6, 11-12. The Board should therefore not credit Dr. Goodrich’s assertions.

Further, there can be no presumption of nexus because PO has not shown that its products are coextensive with the claims, nor could it given PO’s positions in other IPRs that its products embody PO’s other patents that do not mention exfiltration. POR 29, IPR2018-01386, Paper 14 at 63; IPR2018-01443, Paper 12 at 70. Because the ’343 patent does not recite the critical features of these other patents alleged to be embodied in PO’s products, a nexus cannot be presumed. *Fox Factory*, 944 F.3d at 1375 (“A patent claim is not coextensive with a product that includes a ‘critical’ unclaimed feature that is claimed by a different patent.”).

2. The '343 Alleged Invention Was Not The Subject of Industry Praise

PO's purported industry praise also lacks any nexus to the '343 patent claims.

PO's ESG Paper provides nothing more than generalities unrelated to the subject matter of the '343 claims. POR 32–33. Further, PO's attempts to cast generalities in this paper as praising its other patents undercuts PO's assertions that the paper praises the subject matter of the '343 claims. *See* IPR2018-01386 Paper 14 at 61-63; IPR2018-01443 Paper 12 at 68-70. Nor can the self-praising ESG paper “commissioned by Centripetal Networks” be considered *objective* indicia. Ex. 2025, 1. “Such self-generated praise is not persuasive of industry praise.” *Mylan Pharmaceuticals Inc. et al v. Sanofi-Aventis Deutschland GmbH*, IPR2019-00122, Paper 83 at 51 (May 29, 2022); *see also Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01760 Paper 41 at 45, n. 12 (May 18, 2020) (PO commissioning the ESG paper “diminish[es] the persuasive weight it should be accorded.”).

The SINET article also lacks a nexus and says nothing about exfiltration. POR 32-33; Ex. 2028. Dr. Goodrich's assertion that the award is “tied to the technologies in the '343 Patent because they provide techniques for preventing malicious exfiltration” is conclusory and without support. Ex. 2010 ¶115.

The Gartner and American Banker articles likewise lack a nexus. POR 33-34. PO merely recycles text from other IPRs addressing unrelated patents. *E.g.*, IPR2018-01386, Paper 14 at 62; IPR2018-01443, Paper 12 at 69. Both articles recite

generalities, not any purported invention of the '343 patent. Ex. 2027, 5; Ex. 2026, 11–12. Further, the American Banker article reports self-praise from “Steven Rogers, CEO of Centripetal Networks.” Ex. 2026 11.

E. Emerging Threats Is A Printed Publication

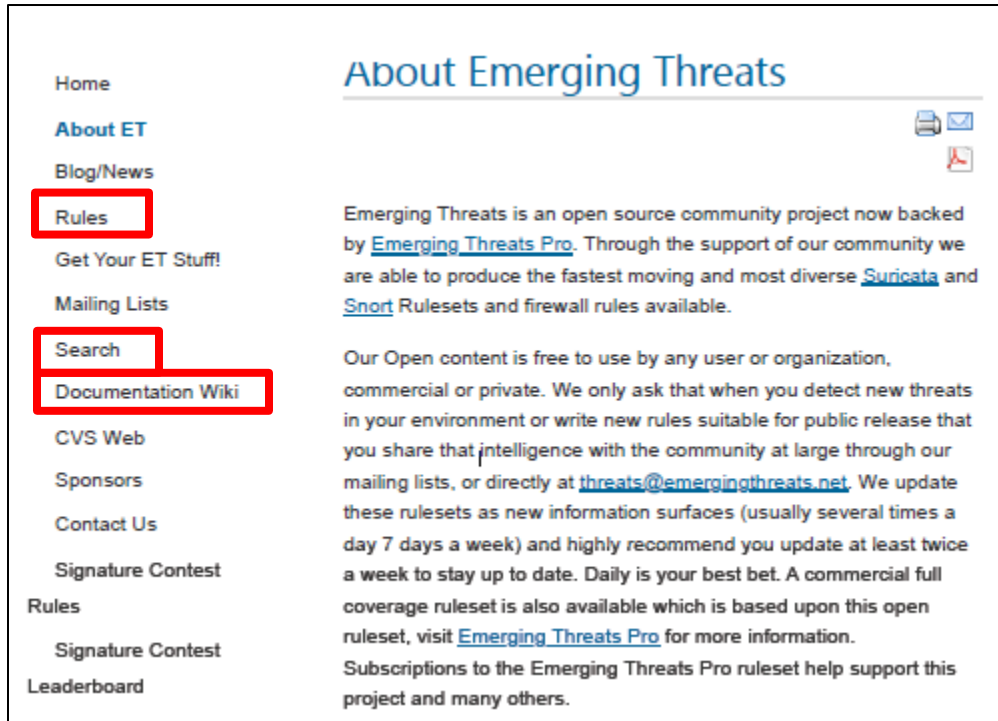
PO argues that Emerging Threats is not a publication because it was purportedly “buried on a website that was not searchable or meaningful[ly] indexed” (POR 34) and that a skilled artisan would have failed to “recognize the relevance” of this reference. POR 36. The record, however, establishes that Emerging Threats was well-known to the relevant public, recognized as the leading third-party distributor of Snort rules, and easily downloaded from the Emerging Threats website.

As the Board recognized in its Institution Decision, “[t]he presence of the Internet Archive’s Wayback Machine copy suggests that the document was available and was accessible on December 2, 2010.” Paper 9 (“I.D.”) 26. The Petition established public availability in view of “Dr. Staniford’s un rebutted testimony that Snort was begun as an open source project in the late 1990s, that the Bleeding Snort project launched in 2004 as an independent clear house for Snort rules, and that the project continues as Emerging Threats.” I.D. 26-27, *citing* EX-1003 ¶¶202-203.

PO’s assertions lack support because rather than analyzing the Emerging Threats website (www.emergingthreats.com) as it existed in 2010 when EX-1020

was archived, PO addresses how the <http://rules.emergingthreats.net> webpage “might have appeared in January 12, 2013.” POR 37. Further, PO’s expert did not recall if he navigated to the archived version of the Emerging Threats website from 2010 or just to the modern version. EX-1100 68:23-69:19; 78:10-19.

The 2010 Emerging Threats website (EX-1102) rebuts PO’s assertions. As annotated below, the website’s left-hand-side included links to the rules, search functionality, and a documentation wiki.



EX-1102 1 (annotated).

Shown below, the website also explains the history from Bleeding Snort, to Bleeding Threats, to Emerging Threats, which corroborates Dr. Staniford's

recollection of Emerging Threats as it was known to those of skill in the art in the 2000s. EX-1003 ¶¶202-203; I.D. 26-27.

Emerging Threats has been in operation under several names since early 2003. We were formed originally as Bleeding Snort, but had to remove Snort from our name several years later for trademark issues. We then became Bleeding Threats. That project had to be abandoned and is defunct unfortunately because of some possible license conflicts that appeared to be arising, so the entire ruleset was moved here, to Emerging Threats. In 2008 we received grant funding from the Army Research Office and the National Science Foundation to continue this project and research. In 2010 Emerging Threats Pro was formed to support this project and offer a complete premium ruleset.

Emerging Threats exists because of the contributions of intelligence and signatures by the community. We give great thanks to the individuals and organizations that have contributed, supported, and made this project possible!

You can download our [rulesets here](#), view our [Documentation Wiki](#), or browse some of the [other excellent projects](#) that have found a home here.

EX-1102 1. The webpage also included a sentence “You can download our rulesets here” with a link to navigate to and download the rule sets. *Id.* An interested artisan could download the rules by navigating the rulesets from those links, as Dr. Staniford did to obtain Emerging Threats, EX-1020. EX-1003 ¶¶204.

The archived website shows that EX-1020 (the emerging-all.rules file) was also accessible through the Ruleset Downloads available through the Documentation Wiki link. As annotated below, the Documentation Wiki allowed users to navigate to Ruleset Downloads, where they could download Exhibit 1020, which included “All Rules in one file.”

The Wayback Machine - <https://web.archive.org/web/20100713225532/http://doc.emergingthreats.net/bin/view/Main/AllRulesets?cover=print>

Ruleset Downloads

All Emerging Threats Signatures

- [emerging-sid-msg-map.txt](#)
- [Browseable Web Directory](#)
- [Last Daily Change Summary](#)
- [SidAllocation](#)
- [Emerging Threats CVS Web Interface](#)

All Rules in one file:

- [emerging-all.rules](#)

All rules and Ancillary Files

- [emerging.rules.tar.gz](#)

Ex. 2016 1 (annotation added).

Further, Mr. Marinho became aware of Emerging Threats through the Snort mailing list while he was an undergraduate student and an intern before 2010. EX-1011 14:15-17:17. He was aware of the Emerging Threats website and personally downloaded the ruleset before 2010:

Q. How did you download the ruleset from Emerging Threats?

A. Navigating through the website and downloading a file that was compressed with all the rule files in it.

...

Q. Did you have any trouble downloading the rules from the Emerging Threats ruleset?

A. No, never had a trouble downloading it. Just as easy as clicking on a link and download, and yes.

EX-1011 17:25-20:12. The ruleset that he easily downloaded was EX-1020:

Q. And when you said prior to your work at Emerging Threats you were able to go to the website and download the all rules, those would have been the open rules; is that correct?

A. That's correct, yes.

Q. This next paragraph, Paragraph 5, refers to the Emerging Threats reference, and then you have the archived URL. It shows "emerging-all.rules." Is that the all rules ruleset that you were referring to before that you would download from the Emerging Threats website?

A. That is right, sir.

Id. 45:11-22.

This shows that an interested artisan exercising reasonable diligence would have been aware of Emerging Threats and known how to download the rules constituting EX-1020.

1. The Emerging Threats Website Made The Rules Available To Persons Exercising Reasonable Diligence

PO's public accessibility argument hinges on assertions that the Emerging Threats website was not "meaningfully indexed" because, according to PO, the Emerging Threats website lacked "any useful scheme or labeling" (POR 39) and lacked "a search function (e.g., a search field or button)." POR 37. PO gets the facts wrong, as explained above. PO's arguments also fail because controlling law requires the availability to interested persons, not indexing. *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 774 (Fed. Cir. 2018) ("The test for public accessibility is not 'has the reference been indexed?'" Instead, the "ultimate

question is whether the reference was ‘available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’”); *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (same). Indexing is not “a necessary condition for a reference to be publicly accessible;” it is one factor that may bear on public accessibility. *Voter Verified, Inc. v. Premier Election Solutions, Inc.*, 698 F.3d 1374, 1380 (Fed. Cir. 2012) (citation omitted). Even for “online references” housed in one corner of the world wide web, the question is whether the reference was “available to the extent that persons interested and ordinarily skilled in the subject matter or art[,] exercising reasonable diligence, can locate it.” *Blue Calypso*, 815 F.3d at 1349.

The Petition showed that Emerging Threats was available to interested persons by 2010. Emerging Threats was a “well-known source of [] custom rules,” including Snort rules, which Dr. Staniford extensively used in the “late 1990s and early 2000s.” EX-1003 ¶¶164, 202, 206. A POSITA would have been “familiar” with Emerging Threats as “source of custom rules” (*id.* ¶164) as they describe a large real-world working system “developed by hundreds of people over more than a decade.” *Id.* ¶199. Mr. Marinho’s personal awareness of the website, recognition of Emerging Threats as the most well-known third-party provider of Snort rules at the time, and access to and use of the rules confirms the reference was available to the interested public. EX-1011 14:15-17:17, 17:25-20:23, 45:11-22.

In sum, a skilled artisan interested in the subject of protecting against cyber-attacks, including exfiltrations, “would have been independently aware” of the Emerging Threats website and could download the rules—Emerging Threats reference EX-1020—“applying reasonable diligence.” *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019), *citing Voter Verified*, 698 F.3d at 1381 (recognizing that a reference was publicly accessible even though there was “no evidence that the reference had been meaningfully indexed or cataloged”).

2. Dr. Staniford's Testimony Is Grounded in Facts

PO rehashes its pre-institution argument that Dr. Staniford's testimony should be afforded “little weight” because it is supposedly “unsupported and omits key dates and details” to show public accessibility. POR 40-41. However, the record now further supports the Board's finding that “one of ordinary skill in the art, at and prior to the effective filing date of the '343 Patent, would have known to look to the Emerging Threats website for Snort rules.” I.D. 27.

As discussed above, the Petition and Dr. Staniford's declaration showed that Emerging Threats was publicly available prior to the critical date. Dr. Staniford explained that Emerging Threats was a “well-known source of [] custom rules,” he was familiar with Bleeding Snort, which became Emerging Threats, and that “a POSA by 2010 would have been familiar with Emerging Threats as a source of

custom rules.” *Id.* ¶¶164, 202, 206; Pet. 19, 35-36. Dr. Staniford’s deposition reinforced his declaration testimony. Ex. 2011 20:14-24. Dr. Staniford explained that he lacked a specific memory of when he first learned of Bleeding Snort because it was a “well-known project in the community.” Ex. 2011 39:23-40:7, 20:14-24:10 (“this is 20 years ago” and he “participated in a variety of mailing lists and conferences and the like about intrusion detection”).

Mr. Marinho’s testimony regarding Emerging Threats being known as Bleeding Edge/Snort more than 13 years ago corroborates Dr. Staniford’s recollection and shows public availability. EX-1101 18:6-21; 22:8-23:13. Mr. Marinho knew of Emerging Threats because it was discussed on the Snort mailing list, acknowledged that it was the most well-known Snort rule provider, and downloaded and used the Emerging Threats rules prior to 2010. *Id.*, 14:15-17:17; 20:19-23; 23:14-24:7.

The Federal Circuit found similar facts sufficient to prove public availability of an online article in *Voter Verified*. Emerging Threats was posted to a website “distributed online via a subscription mailing list,” was “made available for download through” a website, and “became available worldwide on the internet through the website.” 698 F.3d at 1380-1381. Like the *Voter Verified* article, Emerging Threats was “well known to the community interested” in Snort rules and was “treated by the community as public disclosures.” *Id.* Finally, the Emerging

Threats reference was retrievable from the website and “available for download.”

Id. at 138–81; EX-1101 19:13-20:12; 45:11-22. The record here more strongly establishes public availability since Mr. Marinho in fact knew of and downloaded Emerging Threats prior to 2010. EX-1101 45:11-22.

3. A POSITA Would Have Recognized The Relevance of Emerging Threats

PO argues that a POSITA would not have recognized the relevance of Emerging Threats prior to the '343 patent without the need of further research or experimentation because the website lists “thousands of rules” that are “indexed only by a Snort ID (SID).” POR 42-45. PO asserts a “keyword” search would prove “unreasonable” as persons proceeding to the “Emerging Threats website without knowledge of a specific SID ‘would have found [searching by SID] to be of little help.’” POR 43-45, *citing* I.D. 27.

The Board previously rejected this argument, finding that “it would only have required the exercise of reasonable diligence to find the rules list, given the knowledge that ordinary skill would have had regarding Emerging Threats.” I.D. 27. The Board further found that a skilled artisan would “have been able to have searched its contents and find the rules contained thereon.” *Id.* at 28. The record confirms that people like Mr. Marinho who were interested in network security and Snort rules were aware of, downloaded, and used Emerging Threats by 2010.

PO's assertions that a POSITA would have had to perform additional research or experimentation to recognize the relevance of Emerging Threats is baseless. PO's expert admitted to knowing that Sourcefire used Snort rules prior to 2013. EX-1100 15:3-7. Further, Mr. Marinho acknowledged that Emerging Threats was the most well-known third-party supplier of Snort rules, which he downloaded and used before 2010. EX-1101 20:19-23, 23:14-24:7.

PO's argument that SIDs do not provide a meaningful index misses the mark because the issue is whether an interested person could find and access the reference with reasonable diligence. The fact that Emerging Threats was published as a listing of "emerging-all.rules" shows that interested artisans downloaded the entire ruleset and reviewed it to determine which rules they wanted to use. The comments within Emerging Threats evidence this, such as one indicating that "This rule is disabled by default. ... Enable it where useful." EX-1020 at 109 (SID:2001328). Interested persons could easily download Emerging Threats and read the rules and their comments to understand the rules and decide which ones to use.

Further, PO's cited cases (POR 42-44) address whether references qualify as prior art publications, not the ease of locating a specific teaching within a publication. *Cordis Corp. v. Boston Scientific Corp.*, 561 F.3d 1319, 1333 (Fed. Cir. 2009) (addressing whether a limited distribution renders the monographs printed publications); *In re Lister*, 583 F.3d 1307, 1315-16 (Fed. Cir. 2009) (addressing

whether a manuscript could be located exercising reasonable diligence); *Acceleration Bay*, 908 F.3d at 773 (addressing whether a reference that was uploaded to a website could be located using reasonable diligence). The reasoning of these cases confirms that Emerging Threats qualifies as a prior art publication because in 2010 it could be easily located by the interested public. *See supra* § III.E.1.

IV. Conclusion

Petitioner respectfully requests the Board find all claims of the '343 patent unpatentable.

Respectfully submitted,

Date: January 31, 2024

/Gerard M. Donovan/

Gerard M. Donovan

Reg. No. 67,771

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(a) and (d), the undersigned hereby certify that this Reply to Patent Owner's Response complies with the type-volume limitation of 37 C.F.R. § 42.24(c)(1) permitting replies to patent owner responses up to 5,600 words because, exclusive of the exempted portions, it contains 5,579 words as counted by the word processing program used to prepare the paper.

Respectfully submitted,

Date: January 31, 2024

/Gerard M. Donovan/

Gerard M. Donovan

Reg. No. 67,771

Counsel for Petitioner

CERTIFICATE OF SERVICE

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, the undersigned certifies that filing the foregoing **PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE** and Exhibit Nos. 1100, 1101 and 1102 on P-TACTS today constitutes service on the following Patent Owner's representatives:

James Hannah (jhannah@kramerlevin.com)

Jenna Fuller (jfuller@kramerlevin.com)

Jeffrey H. Price (jprice@kramerlevin.com)

Scott M. Kelly (skelly@bannerwitcoff.com)

Bradley C. Wright (bwright@bannerwitcoff.com)

Date: January 31, 2024

/Gerard M. Donovan/

Gerard M. Donovan

Reg. No. 67,771

Counsel for Petitioner