

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.

Petitioner

v.

OPEN TEXT INC.

Patent Owner

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

PATENT OWNER'S PRELIMINARY RESPONSE

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)	2
A.	<i>Fintiv Factor 1: The District Court Has Not Granted And Will Not Grant A Stay</i>	<i>5</i>
B.	<i>Fintiv Factor 2: A District Court Trial Is Expected Before The Projected Statutory Deadline</i>	<i>11</i>
C.	<i>Fintiv Factor 3: The Parties Will Have Invested Significant Resources In The District Court Proceeding</i>	<i>13</i>
D.	<i>Fintiv Factor 4: The Issues Overlap Significantly</i>	<i>15</i>
E.	<i>Fintiv Factor 5: Both Parties Are Parties In The Parallel Litigation</i>	<i>17</i>
F.	<i>Fintiv Factor 6: The Petition Does Not Present Compelling Evidence Of Un-patentability</i>	<i>18</i>
III.	THE '045 PATENT	19
A.	<i>The Prior Art</i>	<i>19</i>
B.	<i>Innovations Of The '045 Patent</i>	<i>21</i>
C.	<i>Claim Construction</i>	<i>23</i>
D.	<i>Level Of Ordinary Skill In The Art</i>	<i>26</i>
IV.	OVERVIEW OF THE RELEVANT PRIOR ART	26
A.	<i>Overview of Rockwood</i>	<i>26</i>
B.	<i>Overview of Xie</i>	<i>30</i>
1.	Anomaly Detection Using Spatiotemporal Correlation	31

2.	Network Forensics Using Spatiotemporal Event Correlation.....	32
V.	THE CHALLENGED CLAIMS ARE PATENTABLE	33
A.	<i>Petitioner Fails To Clearly Articulate A Combination Of Rockwood’s And Xie’s Teachings</i>	34
B.	<i>Petitioner Fails To Establish That Rockwood In View Of Xie Renders Obvious Claims 1–19</i>	39
1.	Rockwood Does Not Disclose Or Render Obvious Gathering Information About Events Defining An Action Of A First Object Acting On A Target.....	41
2.	The Rockwood/Xie Combination Does Not Disclose Or Render Obvious “Generating A Contextual State...” That Includes The Claimed “Originating Object”	49
3.	The Rockwood/Xie Combination Does Not Disclose Or Render Obvious The Claimed “Global Perspective” For A Recited Event That Includes Related Events Across A Network	58
4.	The Rockwood/Xie Combination Does Not Disclose Or Render Obvious The Claimed Event Line	63
5.	A POSITA Would Not Have Been Motivated To Combine Rockwood With Xie Because Each Reference Embodies The Problems Of The Prior Art.....	66
C.	<i>Petitioner’s Grounds Fail To Anticipate Or Render Obvious All Dependent Claims</i>	68
D.	<i>Secondary Objective Indicia Of Nonobviousness</i>	68
VI.	CONCLUSION.....	68

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	<i>passim</i>
<i>Billy Goat Indus., Inc. v. Schiller Grounds Care, Inc.</i> , Case IPR2014-00742, Paper 8 (PTAB Nov. 7, 2014)	62
<i>Cisco Sys., Inc. v. Monarch Networking Solutions LLC</i> , IPR2020-01227, Paper 11 (PTAB Mar. 4, 2021)	13
<i>Commscope Techs. v. Dali Wireless, Inc.</i> , IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023)	19
<i>DeSilva v. DiLeonardi</i> , 181 F.3d 865 (7th Cir. 1999)	38
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	34
<i>Eclinical Works, LLC v. Decapolis LLC</i> , IPR2022-00229, Paper 10 (PTAB Apr. 13, 2022)	12
<i>Ericsson Inc. v. Collision Comms., Inc.</i> , IPR2022-01233, Paper 12 (PTAB Jan. 19, 2023)	15
<i>Google LLC v. EcoFactor, Inc.</i> , IPR2021-00454, Paper 9 (PTAB July 22, 2021)	16
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	34, 66
<i>InfoBionic Inc. v. Braemer Mfg., LLC</i> , IPR2015-01705, Paper 11 (Feb. 16, 2016)	34

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,578,045

<i>Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, slip op. (W.D. Tex. Dec. 22, 2022)	7
<i>Liberty Mutual Ins. Co. v. Progressive Cas. Ins. Co.</i> , CBM2012-00003 Paper 8 (Oct. 25, 2012)	34
<i>Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.</i> , IPR2021-01280, Paper 8 (PTAB Mar. 9, 2022)	35, 66
<i>Luxshare Precision Industry v. Amphenol Corp.</i> , IPR2022-00132, Paper 10 (PTAB May 3, 2022)	10
<i>Lyft, Inc. v. Quartz Auto Techs., LLC</i> , IPR2020-01450, Paper 7 (Mar. 4, 2021)	37, 55
<i>Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.</i> , IPR2019-01445, Paper 12 (Jan. 22, 2020)	12
<i>mCom IP, LLC v. Cisco Sys., Inc.</i> , No. 6:22-00261-ADA, slip op. (W.D. Tex. Oct. 20, 2022)	7
<i>Motorola Mobility LLC v. Ironworks Patents, LLC</i> , IPR2021-00421, Paper 11 (PTAB July 22, 2021)	10
<i>NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018)	12
<i>Nintendo Co. v. Gamevice, Inc.</i> , IPR2020-01197, Paper 13 (PTAB Jan. 12, 2021)	10
<i>Nokia of Am. Corp. v. Godo Kaisha IP Bridge</i> , IPR2022-00755, Paper 9 (PTAB Nov. 2, 2022)	17
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005, Paper 20 (PTAB Aug. 25, 2022)	13
<i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01153, Paper 10 (Jan. 24, 2022)	38

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,578,045

<i>Regeneron Pharmas. Inc. v. Novartis Pharma AG</i> , IPR2020-01317, Paper 15 (PTAB Jan. 15, 2021)	14, 15
<i>Samsung Elecs. Co. v. California Institute of Tech.</i> , IPR2023-00131, Paper 10 (PTAB May 4, 2023).....	12
<i>Samsung Elecs. Co. v. Clear Imaging Research LLC</i> , IPR2020-01399, Paper 13 (PTAB Feb. 3, 2021).....	10
<i>Sonrai Memory Ltd. v. Kingston Tech. Co.</i> , No. 6:21-cv-1284-ADA, slip op. (W.D. Tex. Oct. 18, 2022).....	6
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	16
<i>T-Mobile US, Inc. v. TracBeam LLC</i> , IPR2015-01687, Paper 10 (PTAB Feb. 12, 2016).....	62
<i>United States v. Dunkel</i> , 927 F.2d 955 (7th Cir. 1991)	39
<i>Vizio, Inc. v. Maxell, Ltd.</i> , IPR2022-01459, Paper 7 (PTAB Apr. 11, 2023).....	17
 Statutes	
35 U.S.C. § 312(a)(3).....	34
35 U.S.C. § 314(a)	3, 18
 Regulations	
37 C.F.R. § 42.22(a)(2).....	34
 Other Authority	
H.R. Rep. No. 112-98 (2011), 2011 U.S.C.C.A.N.	1
Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (“Guidance”) (June 21, 2022).....	3, 4, 11, 19

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Nenad Medvidovic, Ph.D
2002	<i>Curriculum Vitae</i> of Professor Nenad Medvidovic, Ph.D.
2003	<i>Webroot, Inc., Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Order Granting Third Amended Scheduling Order, Dkt. 142 (W.D. Tex., Dec. 27, 2022)
2004	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2005	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant’s Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2006	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2007	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. Et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2008	Dani Kass, “Catching Up On Patent Litigation With Judge Albright” (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2009	U.S. District Courts – Federal Court Management Statistics – Profiles – During the 12-month Periods Ending March 31, 2018 Through 2023, “Table N/A – U.S. District Courts – Combined Civil and Criminal

Exhibit	Description
	Federal Court Management Statistics (March 31, 2023),” available https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. Et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Defendant Trend Micro’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2012	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Plaintiff’s Preliminary Infringement Contentions (W.D. Tex., July 13, 2022)
2013	<i>Webroot, Inc. and Open Text Inc., v. Sophos Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Defendant Sophos Ltd.’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2014	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA, Complaint for Patent Infringement, Dkt. 1 (W.D. Tex., Mar. 4, 2022)
2015	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-00241-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 60 (W.D. Tex., Sept. 8, 2022) (excerpted)
2016	<i>Open Text Inc. et al., v. AO Kaspersky Lab</i> , Case No. 6:22-cv-00243-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 80 (W.D. Tex., Oct. 27, 2022)
2017	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 53 (W.D. Tex., Sept. 7, 2022)

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,578,045

Exhibit	Description
2018	<i>Webroot, Inc. and Open Text Inc., v. Sophos, Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Second Amended Complaint for Patent Infringement, Dkt. 76 (W.D. Tex., Oct. 24, 2022)
2019	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-002410ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)

Open Text Inc. ("Patent Owner") submits this Preliminary Response to the Petition of Trend Micro, Inc. ("Petitioner") seeking *Inter Partes* Review ("IPR") of U.S. Patent No. 9,578,045 ("the '045 patent").

I. INTRODUCTION

The Board should decline to institute trial because IPR would duplicate the parties' district court litigation efforts and because the petition relies on an inapposite combination of references, each of which embodies problems the '045 patent addresses and each of which fails to disclose or render obvious all limitations of the challenged claims.

First, the Board should deny institution under *Fintiv* because instituting this IPR would undermine Congress's stated goals in creating IPR proceedings: to provide "quick and cost effective alternatives to litigations" and "limit unnecessary and counterproductive litigation costs." H.R. Rep. No. 112-98, pt. 1, at 40 (2011), 2011 U.S.C.C.A.N. 67, 69. An IPR here would be neither quicker than, nor an alternative to, ongoing district court litigation. The Western District of Texas ("WDTX") is scheduled to proceed to trial on the '045 patent almost three months *before* a final written decision on the petition would be due—so an IPR is not quicker. And, the district court has indicated it will not issue a stay when, as here, it can resolve the same issues prior to the Board—so an IPR is not an alternative to

litigation. Moreover, other defendants have asserted the same prior art raised in the petition, which the district court must address regardless of whether the Board institutes an IPR. Therefore, instituting an IPR would generate the unnecessary and counterproductive litigation costs that Congress sought to avoid.

Second, the Board should deny institution because Petitioner fails to demonstrate a reasonable likelihood that it will prevail on the merits. Petitioner relies on a convoluted web of alternative “mappings” and generalizations about the prior art that fails to clearly articulate a combination of Rockwood’s and Xie’s teachings. Petitioner’s ambiguous petition alone is a sufficient basis to deny institution. Moreover, Rockwood and Xie are directed to very different goals. Rockwood is directed to identifying the human behind a computer attack. Xie is directed to analyzing anomalous file updates and network forensics. These two references do not—alone or in combination—disclose all limitations of the challenged claims. And, even if they did, Petitioner fails to articulate how or why a POSITA would modify Rockwood to incorporate the teachings of Xie.

II. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)

The ’045 patent is one of dozens of patents asserted in claims and counterclaims among six different parties in a series of cases pending in the Western District of Texas. The district court has already issued its claim constructions and is

on track to adjudicate the same prior art raised in the petition months before the Board issues a final written decision. Institution of a parallel IPR proceeding lagging well behind the district court would needlessly increase the cost of resolving the underlying dispute. Under these circumstances, the Board should exercise its discretionary authority to deny institution under 35 U.S.C. § 314(a).

Because Congress's goal in enacting post-grant proceedings like IPRs was "to ... limit unnecessary and counterproductive litigation costs," Director Vidal has instructed the Board not to institute IPRs that would "increase, rather than limit, litigation costs." Director's Memo, *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation* ("Guidance") at 1 (June 21, 2022).

Instituting this IPR would cause just such an increase. A district court stay is out of the question, and the district court will consider the very same prior art presented in the petition. Accordingly, for the next year, the Board and the district court will labor to decide the very same issues with the district court well ahead of—and scheduled to reach a final decision months before—the Board. The year-long parallel tracks of two adjudicatory bodies will "increase, rather than limit, litigation costs," create "potential conflict between the ... (PTAB) and district court proceedings," and generally increase "the potential for inefficiency and

gamesmanship.” Guidance at 1. This is precisely the situation that Director Vidal sought to avoid when she instructed the Board to take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 6 (PTAB Mar. 20, 2020).

Confirming this conclusion, every one of the *Fintiv* factors weighs for discretionary denial:

(1) A stay of the co-pending district court litigation—involving thirty-nine patents and five defendants—is vanishingly unlikely. Petitioner cannot avoid that trial because it has petitioned for review of only five of the eleven patents asserted against it. And this IPR will similarly not narrow the issues on which discovery and trial must proceed—the ’045 patent is currently asserted against four defendants in a now-consolidated case. Moreover, none of Petitioner’s codefendants have agreed not to litigate the validity of the ’045 patent in the district court if the Board institutes this IPR.

(2) Trial in the district court is expected almost three months *before* a final written decision. The district court case remains on track. The claims of the ’045 patent have been construed, and discovery is well underway.

(3) The parties and district court have already invested heavily in carrying the parallel litigation past claim construction—eight months before any anticipated institution decision—and well into discovery.

(4) The issues raised in the petition are the same as those the district court has before it, and Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same grounds* asserted in its petition during the pendency of any IPR instituted from that petition, irrespective of the Board's institution decision.

(5) Petitioner will get its chance to make its arguments before the district court because Petitioner is a defendant in the parallel litigation.

(6) As shown below, the petition's grounds of unpatentability are weak. Thus, every *Fintiv* factor here weighs for discretionary denial. The district court is well on its way to an efficient resolution of the disputes between Patent Owner, Petitioner, and Petitioner's codefendants. Both the goals of the AIA and the general welfare of the patent system would be best served by denying institution.

A. *Fintiv* Factor 1: The District Court Has Not Granted And Will Not Grant A Stay

The first *Fintiv* factor asks “whether [1.] the court granted a stay or [2.] evidence exists that one may be granted if a proceeding is instituted.” *Fintiv*,

IPR2020-00019, Paper 11 at 6.¹ Here, the undisputed answer to both questions is *no*: no stay has been requested or ordered, and Petitioner has identified no evidence that one will (or even might) be. To the contrary, specific evidence indicates that a stay is unlikely.

First, the district court considers issue simplification “the most important factor” in deciding whether to stay patent litigation²—and here, a stay would not

¹ The decision in *Fintiv* addresses various scenarios that may indicate whether a stay may be granted. *Fintiv*, IPR2020-00019, Paper 11 at 6-9. However, nothing in *Fintiv* suggests that these are the only scenarios that a panel may consider. In particular, *Fintiv* does not hold that an actual denial of a stay is the only consideration relevant to this factor. Rather, *Fintiv* contemplates that any type of evidence may be relevant. For example, *Fintiv* holds that one way to “support the arguments that ... a stay may be less likely, and instituting would lead to duplicative costs” is to show the “work completed by the parties and court in the parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 11 at 10.

² See, e.g., EX-2004, *Sonrai Memory Ltd. v. Kingston Tech. Co.*, No. 6:21-cv-1284-ADA, slip op. at **4-5 (W.D. Tex. Oct. 18, 2022) (denying a stay following IPR institution because issue simplification was the “most important factor” and the

simplify anything. The validity of the '045 patent will be litigated in the consolidated district court action, whether this petition is instituted or not, because the patent is asserted against three other defendants, none of whom have promised not to pursue invalidity in the district court based on this institution decision.

Moreover, the validity of the '045 patent will be litigated in the district court alongside issues regarding **38 other** patents asserted by and against Petitioner and **four other** defendants—issues that the district court is highly unlikely to delay deciding in favor of letting the Board proceed with this IPR. The case against Petitioner alone involves nineteen patents—thirteen asserted by Patent Owner and six asserted in counterclaims by Petitioner.

Court had already held a *Markman* hearing and “expended significant resources”); EX-2005, *mCom IP, LLC v. Cisco Sys., Inc.*, No. 6:22-00261-ADA, slip op. at *5 (W.D. Tex. Oct. 20, 2022) (finding “simplification is not likely” where the IPR did not challenge all of the claims asserted in the district court, since the other claims would still require a trial); EX-2006, *Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, slip op. at *7 (W.D. Tex. Dec. 22, 2022) (denying a stay following IPR institution, as even IPR estoppel would not simplify the invalidity case, given the defendants’ reliance on prior art systems).

The table below illustrates the patents, parties, and IPR petitions involved in this highly complex litigation:

**Table 1. Patent Owner's Asserted Patents
Against Each WDTX Defendant and Resulting Review Petitions**

Patent	Kaspersky	CrowdStrike	Forcepoint	Sophos	Trend Micro
9,578,045	IPR2023-01199	IPR2023-00124	<i>N/A</i>	Asserted; no IPR	IPR2023-00677
8,201,243	Asserted; no IPR	IPR2023-01052	Asserted; no IPR	IPR2023-00731	Asserted; no IPR
8,719,932	Asserted; no IPR	IPR2023-01051	Asserted; no IPR	IPR2023-00732	Asserted; no IPR
8,418,250	Asserted; no IPR	IPR2023-00289	<i>N/A</i>	IPR2023-0699	IPR2023-00655
8,726,389	Asserted; no IPR	IPR2023-00556	Asserted; no IPR	IPR2023-00633	Asserted; no IPR
10,599,844	Asserted; no IPR	Asserted; no IPR	Asserted; no IPR	IPR2023-00528	IPR2023-00662
9,413,721	<i>N/A</i>	<i>N/A</i>	Asserted; no IPR	IPR2023-00491	<i>N/A</i>
10,257,224	IPR2023-01011	IPR2023-00126	<i>N/A</i>	Asserted; no IPR	IPR2023-00657
10,284,591	IPR2023-00895	IPR2022-01522	<i>N/A</i>	Asserted; no IPR	IPR2023-00692
8,856,505	Asserted; no IPR	IPR2023-01159	<i>N/A</i>	Asserted; no IPR	Asserted; no IPR
8,181,244	<i>N/A</i>	IPR2023-01158	<i>N/A</i>	Asserted; no IPR	Asserted; no IPR
11,409,869	IPR2023-01160	IPR2023-01053	Asserted; no IPR	PGR2023-00031	Asserted; no IPR
8,763,123	<i>N/A</i>	IPR2023-1050	<i>N/A</i>	Asserted; no IPR	<i>N/A</i>
8,438,386	<i>N/A</i>	<i>N/A</i>	IPR2023-00784	<i>N/A</i>	<i>N/A</i>

Patent Owner's Preliminary Response
to Petition for *Inter Partes* Review
Patent No. 9,578,045

Patent	Kaspersky	CrowdStrike	Forcepoint	Sophos	Trend Micro
10,025,928	N/A	N/A	IPR2023-00786	N/A	N/A

As U.S. Magistrate Judge Gilliland noted during a December 9, 2022 hearing, this is “a phenomenal case that I’m hoping one day maybe people will write songs about because it is about as complicated as you’re going to get with patent cases.” (EX-2007 52.)

Second, the district court has been clear in public comments that it will not stay cases where, as here, the court can resolve the case as quickly as the Board can:

[T]here’s no unfairness to either side by not staying a case for the PTAB when I can try the case as quickly as they can resolve it.... And so far, I think that’s proven to be true.

(EX-2008 3.) Indeed, as commentators have observed, “Judge Albright almost never stays proceedings to let the PTAB make its decision first.” (*Id.* 2.)

Judge Albright’s public comments apply squarely to the situation here. The median time-to-trial in WDTX is 28.2 months. (EX-2009 37.) On that timeline, trial is expected in this case in mid-July 2024. Trial is currently scheduled for August 2024. (EX-2003 6.) The deadline for a final written decision in an IPR here would not be until many months later (in November 2024). That Judge Albright has made public comments indicating that his practice is to deny a stay in precisely the

circumstances presented here is further evidence that he would not stay the WDTX case in response to institution of this IPR.

Even where no stay has been requested, the Board has found Factor 1 to favor discretionary denial where (as here) “Petitioner present[ed] no evidence that it has requested a stay [] or that a stay is likely.” *Luxshare Precision Industry v. Amphenol Corp.*, IPR2022-00132, Paper 10, at 9 (PTAB May 3, 2022). And such a decision is particularly appropriate where the circumstances show that “a stay ... is unlikely.” *Nintendo Co. v. Gamevice, Inc.*, IPR2020-01197, Paper 13, at 11-12 (PTAB Jan. 12, 2021); *Samsung Elecs. Co. v. Clear Imaging Research LLC*, IPR2020-01399, Paper 13 at 11-12 (PTAB Feb. 3, 2021) (holding Factor 1 may weigh for denial where there is evidence that the district court is unwilling “to avoid duplicative efforts and await the PTAB’s final resolution”); *Motorola Mobility LLC v. Ironworks Patents, LLC*, IPR2021-00421, Paper 11 at 7-8 (PTAB July 22, 2021).

In sum, the district court has not granted a stay and there is no evidence suggesting that the district court would grant a stay of a multi-patent, multi-defendant case so that the Board can reach a decision months *after* the current trial date on *just one* patent. Factor 1 weights in favor of discretionary denial. *Samsung*, IPR2020-01399, Paper 13 at 11-12; *Motorola*, IPR 2021-00421, Paper 11 at 7-8.

**B. *Fintiv* Factor 2: A District Court Trial Is Expected Before The
Projected Statutory Deadline**

Factor 2—the implications of the district court and IPR schedules—also weighs for denial. “[A] parallel proceeding in an advanced state implicates considerations of efficiency and fairness, which can serve as an independent reason to apply discretion to deny institution.” *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 11-12, 17 (PTAB May 13, 2020) (*informative*); Guidance at 1.

Here, an IPR would overlap almost entirely with the parallel district court litigation. WDTX’s median time-to-trial is 28.2 months (EX-2009 37), indicating a trial by mid-July 2024—a date consistent with the currently scheduled trial date of August 19, 2024. (EX-2003 6.) Should the Board institute, its final written decision deadline would be November 10, 2024, nearly three months *after* the scheduled trial date. Petitioner asserts that “trial is currently set for August 19, 2024, so there is time to complete inter parte [sic] review” (Petition 67), but that is incorrect. Applying *either* the trial date set by the Court *or* WDTX’s median time-to-trial, an *Inter Partes* Review would not be complete before the ’045 patent’s validity is resolved at trial in WDTX.

In other words, if the Board institutes an IPR here, the IPR proceedings would not produce a result before the trial, and the parties would spend a year expending precisely the “duplicative,” “unnecessary[,] and counterproductive litigation costs”

that the AIA was designed to avoid. *Fintiv*, IPR2020-00019, Paper 11 at 5 (citing *Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.*, IPR2019-01445, Paper 12 at 10 (Jan. 22, 2020)); *see id.*, Paper 15 at 17 (discretionarily denying institution where district court trial was scheduled two months before the final decision deadline); *NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (*precedential*) (finding that institution of IPR when the district court trial would resolve validity before the PTAB “would not be consistent with an objective of the AIA...to provide an effective and efficient alternative to district court litigation”); *Samsung Elecs. Co. v. California Institute of Tech.*, IPR2023-00131, Paper 10 at 15, 24 (PTAB May 4, 2023) (discretionarily denying institution where “[r]egardless of whether we consider the scheduled trial date or the trial date expected based on time-to-trial statistics, the trial in the underlying litigation would commence several months before the expected date of our final written decision”); *Eclinical Works, LLC v. Decapolis LLC*, IPR2022-00229, Paper 10 at 9 (PTAB Apr. 13, 2022) (discretionarily denying institution where WDTX trial was scheduled “roughly one to two months before any final decision would have been due”).

Because the district court will resolve validity before the Board reaches its final written decision, the second *Fintiv* factor also favors discretionary denial.

C. *Fintiv* Factor 3: The Parties Will Have Invested Significant Resources In The District Court Proceeding

Factor 3—the resources invested in the parallel district court proceeding—favors denial “if, at the time of the institution decision, the district court has issued substantive orders related to the patent.” *Fintiv* at 9-10; *see also id.* at n.16 (collecting cases). *Fintiv* holds specifically that “claim construction orders may indicate that the court and parties have invested sufficient time in the parallel proceeding to favor denial.” *Id.* at 10.

The parties have invested significant resources in the parallel litigation over the last eighteen months. For example, the parties long ago exchanged infringement and invalidity contentions (in July 2022 and September 2022 respectively), and fact discovery is underway. Claim construction, too, is long since complete. (EX-2010.)

And while *Fintiv* directs consideration of resource investment at the time of institution, the overlapping schedules here counsel the Board to further consider the redundant resources that ***will be*** wasted should IPR be instituted. *Id.* at 6; *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 20 at 7 (PTAB Aug. 25, 2022) (Board should consider “the duplicative efforts that will occur during the [] duration of a [inter partes] review”); *Cisco Sys., Inc. v. Monarch Networking Solutions LLC*, IPR2020-01227, Paper 11 at 11-12 (PTAB Mar. 4, 2021) (finding that more work

completed by the parties and the court suggests that institution would lead to duplicative costs).

The investment in this case is colossal. The district court's *Markman* order that included the '045 patent was twenty pages, without even considering the Court's substantive analysis or the additional *Markman* orders issued in this case. (EX-2010.) The Court considered and construed four claim terms of the '045 patent, alone. (*Id.* 8-10.) And, the parties have engaged in extensive discovery on the parties' contentions, during which Patent Owner has made approximately 50TB of source code available. The Court has held multiple discovery hearings. Furthermore, Petitioner's and Patent Owner's experts have already invested an extensive number of hours preparing for their reports by reviewing the patent, prior art, and Defendants' invalidity contentions, as well as traveling to review source code for more than two months. *See Regeneron Pharms. Inc. v. Novartis Pharma AG*, IPR2020-01317, Paper 15 at 17 (PTAB Jan. 15, 2021) (discretionarily denying institution where the parties had expended considerable resources in claim construction, substantial fact discovery, and preparation for expert reports).

Petitioner's delay in filing this petition further weighs for denial. Petitioner waited almost exactly twelve months after receiving Patent Owner's March 4, 2022 complaint, eight months after receiving Patent Owner's infringement contentions,

and six months after serving its invalidity contentions before filing its petition. (EX-2014; EX-2012 1-2; EX-2011 1-2.) Petitioner offers no explanation for its delay, which weighs for denial. *Fintiv*, IPR2020-00019, Paper 11 at 11-12; *Ericsson Inc. v. Collision Comms., Inc.*, IPR2022-01233, Paper 12 at 15 (PTAB Jan. 19, 2023) (finding that where the parties invested significant resources and “Petitioner waited almost a year” to file its petition, “this factor weighs decidedly in favor of discretionary denial”); *Regeneron*, IPR2020-01317, Paper 15 at 17 (finding that even where the petition was filed “less than a month after learning of the complaints,” the investment by the parties in the parallel proceeding “outweighs the effort expended so far in this proceeding”).

D. *Fintiv* Factor 4: The Issues Overlap Significantly

Factor 4—the degree of overlap between the issues in the petition and those before the district court—also strongly supports denial.

Regarding this fourth factor, *Fintiv* explains that “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong” where “the Board [is] presented with substantially identical prior art arguments...at issue in district court.” *Fintiv*, IPR2020-00019, Paper 11 at 12. “Accordingly, if the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.” *Id.*

Here, Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments based on precisely the same grounds* asserted in its petition during the pendency of any IPR. Even if Petitioner had offered a stipulation, such a stipulation would carry no weight because it does not bar the other defendants in the parallel litigation from litigating the very same invalidity challenges before the district court. Petitioner's co-defendants are collectively relying in the litigation on the same prior art asserted in the petition.³ In light of the inevitable parallel tracks, instituting an IPR would not only multiply the burden on Patent Owner, it would also create the possibility of inconsistent decisions between the district court and the Board.

Because Petitioner makes no effort to “mitigate[] any concerns of duplicative efforts between the district court and the Board,” or “of potentially conflicting decisions,” Factor 4 weighs heavily in favor of discretionary denial. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 19 (PTAB Dec. 1, 2020); *Google LLC v. EcoFactor, Inc.*, IPR2021-00454, Paper 9 at 12-14 (PTAB July 22, 2021).

³ Codefendant CrowdStrike and Sophos each assert Rockwood and Xie. (EX-2019 10-11; EX-2013 31-32.)

E. *Fintiv* Factor 5: Both Parties Are Parties In The Parallel Litigation

Factor 5—the overlap of the parties between the petition and the parallel litigation—suggests denial because (1) Petitioner is a defendant in the parallel litigation and, as such, will have a full, fair opportunity to litigate the petitioned grounds, and (2) the issues Petitioner raises are the same ones its co-defendants have *also* raised in the parallel litigation.

Under *Fintiv*, “[i]f a petitioner is unrelated to a defendant in an earlier court proceeding, the Board has weighed this fact against exercising discretion to deny institution.” *Fintiv*, IPR2020-00019, Paper 11 at 13-14. That is not the case here because Petitioner is a defendant in the litigation. Accordingly, the circumstances raise no fairness concerns that denial would deprive Petitioner of its “day in court.” *See Vizio, Inc. v. Maxell, Ltd.*, IPR2022-01459, Paper 7 at 21-22 (PTAB Apr. 11, 2023) (“Because Petitioner is the litigation defendant, factor 5 weighs in favor of discretionary denial”); *Nokia of Am. Corp. v. Godo Kaisha IP Bridge*, IPR2022-00755, Paper 9 at 13 (PTAB Nov. 2, 2022) (holding that Factor 5 weighed for discretionary denial where Petitioner was defendant in parallel proceeding).

That other defendants are *also* litigating the petitioned issues at the district court further suggests denial. *Fintiv* holds that, “[e]ven when a petitioner is unrelated to a defendant, however, if the issues are the same as, or substantially similar to,

those ... about to be litigated, or other circumstances weigh against redoing the work of another tribunal, the Board may, nonetheless, exercise the authority to deny institution.” *Id.* at 14. Because of this consideration, *Fintiv* goes on to require that “[a]n unrelated petitioner ... discuss why addressing the same or substantially the same issues would not be duplicative of the [other] case even if the petition is brought by a different party.” *Id.*

Petitioner offers no such explanation here. That other defendants are currently litigating the same issues raised in the petition raises serious concerns of duplicative work by adjudicators, and any public-policy concerns regarding patent validity will be thoroughly addressed by the parallel litigation. Thus, that *other* defendants in the district court proceedings are *also* litigating the petitioned grounds weighs yet further for discretionary denial.

F. *Fintiv* Factor 6: The Petition Does Not Present Compelling Evidence Of Un-patentability

Factor 6—the merits of the Petition—also weighs against institution because, as detailed below, the petition fails to show a “reasonable likelihood” that Petitioner would prevail on any challenged claim. *See* 35 U.S.C. § 314(a). The petition fails to articulate the combination with adequate clarity. And, to the extent Petitioner’s arguments can be discerned, Petitioner’s proposed combination is exceptionally

weak. *See* Section IV, *infra*. Because the petition fails to show a reasonable likelihood of success on the merits, the petition may not be instituted.

Even if the petition did have a “reasonable likelihood” of succeeding (it does not), it certainly would not pass the higher threshold of a “compelling” unpatentability challenge that could preclude discretionary denial. Guidance at 4. “[T]he compelling merits standard is a higher standard than the standard for institution set by statute.” *Commscope Techs. v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 at 3 (PTAB Feb. 27, 2023). That higher standard requires determining that Petitioner is “*highly* likely” to succeed on the merits. *Id.* at 4. The opposite is true here.

* * *

In sum, all six factors weigh for discretionary denial. Accordingly, Patent Owner respectfully requests that the Board exercise its discretion to deny institution.

III. THE '045 PATENT

A. The Prior Art

At the time of the invention of the '045 patent, network forensics systems used network forensics tools, e.g., network sniffers and packet capture tools, to detect and capture information associated with communication sessions. (*See* EX-1001 1:24-33; EX-2001 ¶28.) Such network forensics tools passively collect network traffic

and reside at a network edge, e.g., a location where an organization's network interfaces with the internet. (See EX-1001 1:33-43; EX-2001 ¶28.) Although network edge devices may receive network events, they cannot establish any sort of contextual information about the event from within the host or system generating the event. (See EX-1001 1:40-43; EX-2001 ¶28.)

As a result, network forensics tools could not obtain useful information from within a host or establish any sort of context with information about the event from within a host that was generating and/or receiving network events. (See EX-1001 1:36-48; EX-2001 ¶29.) Without this information, prior art network forensics tools were insufficient to identify and address threats faced by modern computer networks. (See EX-1001 1:46-49; EX-2001 ¶29.) Although a network edge device may be able to monitor, capture, and analyze communications traffic, the network edge device could not provide details regarding files modified, registry entry changes, or new processes created within the network core. (See EX-1001 1:63-2:12; EX-2001 ¶30.) The network edge device thus had no way of knowing to what extent a virus may have impacted computing devices on the network, what additional files may have become infected, or what operating processes and/or objects are linked to the virus. (See EX-1001 2:12-16; EX-2001 ¶30.)

B. Innovations Of The '045 Patent

The '045 patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks” and describes and claims a system and method that improved on traditional network forensics tools used to discover or identify security issues on computer networks. (EX-1001 Abstract, 1:1-18, cls. 1, 8, 16.)

Unlike traditional network forensics tools, the '045 patent creates forensic visibility *into* the computing devices on the communication network to identify malware or other security issues in the operation of those devices. (EX-1001 2:31-38.) In particular, the '045 patent improves network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event, generating an “event line” comprising information relating to the “event,” and transmitting the generated “event line” that includes information for the event. (See EX-1001 cls. 1, 8, 16.) The described and claimed systems and methods collect endpoint events, create audit trails for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establish a global perspective of the objects. (EX-1001 1:16-18, 3:45-49, 8:30-37, 12:59-63, 18:55-57; EX-2001 ¶33.)

In addition to analyzing the behavior of objects to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (EX-1001 2:39-42; *see also* EX-2001 ¶34.) The '045 patent implements a “context analyzer” to ensure that a user, such as a network administrator, is provided the deepest view of the most important data but still has access to the full range of data if they wish to see it. The analysis starts by correlating events to objects (their originating processes, devices, and users) and creating an audit trail for each event. This allows an administrator to forensically track back any event which occurs to what triggered it. As previously discussed, conventional products in this space receive events outside of the system (for example, as a network edge device) and therefore have no ability to establish context within the system. (EX-1001 3:41–49.) In many cases, a potentially malicious object is identified by the system as a result of other events that provide information relevant to whether the code is malicious. (EX-2001 ¶34.)

The '045 patent further explains that, in addition to contextual information, the patented systems and techniques can also use information from the network to obtain a global perspective of the network's operation. (EX-1001 3:59–4:7; EX-2001 ¶35.) The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or

similar objects) that have been identified previously as malicious. (EX-1001 8:65–9:3; EX-2001 ¶35.) As malicious code and threats evolve more quickly, this combined approach improves detection time and enhances overall network security. (EX-1001 2:16-19, 23-38, EX-2001 ¶35; *see* EX-1001 2:47-53, 3:23–28 3:55-57, 8:9-19.)

The '045 patent further discloses technical improvements to forensics systems by “assembling” or “generating” an “event line” based on the contextual information and global perspective. (EX-1001 9:50–58.) The generation of the event line makes it easier for end users to “identify events, and/or instances of malware, that require more immediate attention”—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and address any damage inflicted by an originating object. (EX-1001 9:45–49.)

C. Claim Construction

Petitioner does not identify any dispute over the construction of claim terms for the purposes of its petition. (Petition 9.) On March 16, 2023, the district court concluded that no terms of the '045 patent were indefinite. (EX-2010 8-11.) In its claim construction order, the Court construed certain limitations of the '045 patent as follows:

Claims	Claim Term	Court's Construction
1	"wherein the global perspective for one or more related events to the at least one event across a network"	Not indefinite "wherein the global perspective [is] for one or more related events to the at least one event across [other devices on] a network"
14	"global perspective"	Not indefinite. Plain-and-ordinary meaning wherein the plain-and-ordinary meaning is "information about events related to the monitored even [sic] ⁵ across a network"

⁴ The Court's claim construction order only construes "global perspective" for claim 1. (EX-2010 8.) Because "global perspective" also appears in independent claims 8 and 16 and the petition provides no basis for applying a different meaning of "global perspective" for those claims, Patent Owner applies the Court's construction for "global perspective" in claim 1 for all claims that recite a "global perspective" limitation.

⁵ Patent Owner understands "even" in the Court's claim construction order as a typographical error that should instead recite: "event."

Claims	Claim Term	Court's Construction
1 ⁶	"event line"	Plain-and-ordinary meaning.
1, 8, 16	"gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device; generating contextual state information for the event by correlating the event to an originating object of the first object; obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and	No order of steps required

⁶ The Court's claim construction order only construes "event line" for claim 1. (EX-2010 8.) Because "event line" is also recited by independent claims 8 and 16 and the petition provides no basis for applying a different meaning of "event line" for those claims, Patent Owner applies the Court's construction for "event line" in claim 1 for all claims that recite an "event line" limitation.

Claims	Claim Term	Court's Construction
	wherein the global perspective relates to one or more other events related to the event across a network”	

In this preliminary response, Patent Owner and its expert apply the Court's construction for all construed terms and the plain and ordinary meaning of the claim terms that the Court did not construe. (EX-2001 ¶38.)

D. Level Of Ordinary Skill In The Art

A POSITA at the time of the invention of the '045 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2–3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security. (EX-2001 ¶40.) More advanced degrees and/or training in a related discipline can compensate for shorter work experience. (EX-2001 ¶40.)

IV. OVERVIEW OF THE RELEVANT PRIOR ART

A. Overview of Rockwood

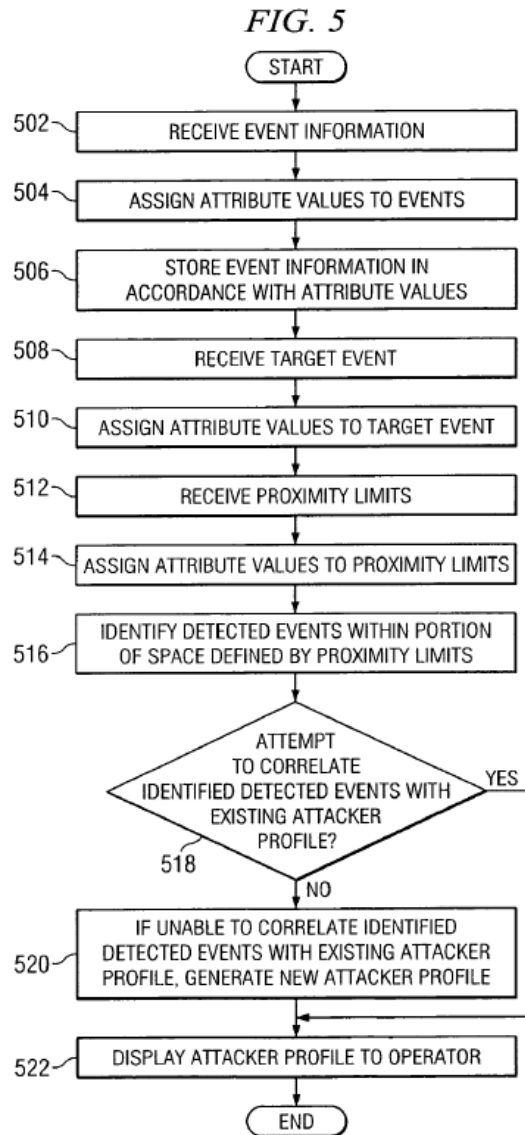
Rockwood is directed to identifying human attackers associated with detected suspicious events. (EX-1004 14:7-10; EX-1002 ¶121 (“Rockwood explains that the detected event can also be correlated to an attacker profile in an attempt to identify

a human actor associated with the suspicious activity”), ¶125 (“Rockwood discloses providing details on human attackers, such as physical addresses, in attacker profiles.”); EX-2001 ¶44.)

Rockwood performs data collection with a hardware configuration that uses network edge sensors located at a network port that receives TCP/IP packets or other similar communications from network 100. (*See, e.g.*, EX-1004 2:40-45, 3:36-41, 14:52-57, Fig 1, Fig. 6; *see also* EX-2001 ¶45.)

Rockwood's configuration matches the prior art system discussed in the '045 patent, where sensors (e.g., network sniffers) are located at network edges, monitoring traffic without the capability to link into network endpoints. (*Compare* EX-1004 3:36-49 (“Each sensor 20 is located at a network port that receives TCP/IP packets or other similar network communications from network 100. These packets and similar network communications received by sensors 20 are referred to as detected events 110.”) *with* EX-1001 1:36-51 (“[E]xisting network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system.”).)

Like the network sniffer prior art techniques described in the '045 patent, Rockwood's sniffers do not collect information from within endpoints regarding an observed event. (EX-2001 ¶¶46-50.) In addition, Rockwood's event processing does not include contextual state information, such as the originating event of an observed event, and does not create an event line. (EX-2001 ¶¶46-50.) Rather, Rockwood processes events in isolation and does not trace a computer object's chain of events within an endpoint. (EX-2001 ¶¶46-50.) Rockwood's event information processing is illustrated by Figure 5:



(EX-1004 Fig. 5.)

Rockwood includes a correlation engine that “is communicatively connected to a memory module 150” that “stores detected events 110 received by sensors 20 for later processing, retrieval, or searches.” (EX-1005 5:1-4.) The correlation engine

“is operable to process event information of detected events 110 stored in memory module 150 to detect the presence of a substantially long-term or multi-staged attack that had previously gone undetected by servers 20 and manager servers 30.” (EX-1005 5:10-14.) The correlation engine “processes each detected event 110 according to the attributes of that detected event” and “uses rules stores in ruleset 152 to determine which attribute values 420 to assign to a particular detected event 110.” (EX-1005 5:66–6:9; *see also id.* at 6:27-62.)

As addressed above, the goal of the correlation process in Rockwood is to identify a *human* attacker profile. (Ex. 1002 ¶121 (“Once the detected event is identified as being within the proximity limits Rockwood explains that the detected event can also be correlated to an attacker profile in an attempt to identify a human actor associated with the suspicious activity: ‘correlation engine 140 attempts to correlate identified detected events 222 with at least one existing attacker profile 224a in profile set 156.’” (quoting EX-1004 14:7-10).)

B. Overview of Xie

Xie is a Ph.D thesis titled “A Spatiotemporal Event Correlation Approach to Computer Security.” (EX-1005 3.) Xie addresses two separate applications of spatiotemporal event correlation: anomaly detection and network forensics. (*Id.*) Anomaly detection evaluates file changes within a given computer and uses those

file changes to identify patterns of file updates that are shared across multiple hosts. (*Id.*) In contrast, network forensics focuses on identifying the host device (e.g., computer) through which an attack entered the network and the flow of the attack to other host devices. (*Id.*)

1. Anomaly Detection Using Spatiotemporal Correlation

In Xie's anomaly detection technique, the "state change" of a given computer (also referred to in Xie as "state transition") is abstracted into an n-dimensional point and may be used to create an n-dimensional vector. (EX-1005 1, 25-26 ("The correlation is performed by clustering points, each representing an individual host state transition due to one or more file system changes, in a multi-dimensional feature space. Each feature indicates the change of a file attribute, with all features together describing the host state transitions of an individual machine during a given period (e.g., one day)."), 29-30, 33.)

Xie uses file system updates to represent host state changes for its anomaly detection technique. (EX-1005 25-26, 30-31; *see also id.* at 131 ("In Seurat, we use file system update events to represent host state changes and thus require per-host based monitoring. With the increasing deployment of network traffic monitors, we can easily log both the incoming and outgoing traffic of each host without interfering normal host functions.")) Xie's technique "identifies anomalies **without**

foreknowledge of normal changes and without system-specific knowledge” by examining “both the temporal and spatial locality of host state changes in a network system.” (EX-1005 30 (emphasis in original).)

Xie's anomaly detection does not identify the originating file/object or process of any instance of detected malware and does not assemble an event line. (EX-2001 ¶¶52-55.) Xie references identifying a list of “suspicious” files associated with anomalous changes, but does not identify any object that originates any other object. (EX-1005 48; EX-2001 ¶¶53-55.)

2. Network Forensics Using Spatiotemporal Event Correlation

Xie's network forensics technique aims to identify the “true source” of an internet attack (i.e., the computer or network that launched the attack). (EX-1005 59.) Many types of internet attacks use indirection as a means to hide their source. (EX-1005 59.) For example, using a chain of compromised machines, or “stepping stones,” is a common means of foiling a defender's attempts to locate the source of an attack. (EX-1005 59-60.) Similarly, distributed denial-of-service (DDoS) attacks are often launched from compromised computers, sometimes called “zombies,” both to harness the power of many machines and to obfuscate where the true source of the attack lies. (EX-1005 59-60.)

Xie’s identification process includes collecting network traffic *between computers* that are being monitored and performing Monte Carlo sampling (e.g., random walk algorithm) to reveal the “initial attack path” that leads to the true source computer. (See, e.g., EX-1005 59-60.) Xie’s network forensics technique generates a *causal tree* between *different computers* in a network. (See, e.g., EX-1005 61-63, Figs 3.2 (example of host contact graph showing an attack spread between hosts), 3.3 (where each oval represents a host node).) This is unlike the ’045 patent, which looks at different computer objects within a given computer—not different host nodes, i.e., computers. (EX-2001 ¶¶31–34, 55-58.)

To collect all network traffic among different nodes, Xie teaches the use of sensors or “auditing devices” for the intrusion detection system’s traffic logging. (EX-1005 64-66; *see also* 77-78, Figure 3.12 (collecting traffic “from the *backbone* of a university network”); EX-2001 ¶¶56-59.) In this aspect, the architecture of network forensics in Xie is similar to that of Rockwood, and they suffer similar deficiencies, including the inability to look inside endpoints to collect contextual information around an observed event. (EX-2001 ¶59.)

V. THE CHALLENGED CLAIMS ARE PATENTABLE

Petitioner seeks *Inter Partes* Review of the ’045 patent on one ground:

Ground 1	Section 103	Obvious over Rockwood in view of Xie	Claims 1-19
-----------------	-------------	---	-------------

**A. Petitioner Fails To Clearly Articulate A Combination Of
Rockwood's And Xie's Teachings**

“In an inter partes review, the burden of persuasion is on the petitioner.... Failure to prove the matter as required by the applicable standard means that the party with the burden of persuasion loses on that point—thus, if the fact trier of the issue is left uncertain, the party with the burden loses.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (noting petitioners have the “burden from the onset to show with particularity why the patent it challenges is unpatentable”). A petition must include “a detailed explanation of the significance of the evidence.” *See* 37 C.F.R. § 42.22(a)(2); *see also* 35 U.S.C. § 312(a)(3).

A petition that fails to articulate clearly how a proposed combination should be effected is alone a sufficient basis to deny institution. *See InfoBionic Inc. v. Braemer Mfg., LLC*, IPR2015-01705, Paper 11 at 11 (Feb. 16, 2016) (denying institution where petitioner failed to “articulate adequately to what extent and how [p]etitioner proposes [first prior art’s] method would be incorporated into [second prior art’s] system,” leaving the Board to “speculate as to how [p]etitioner’s combination of references’ teachings would render obvious” the challenged claims); *Liberty Mutual Ins. Co. v. Progressive Cas. Ins. Co.*, CBM2012-00003 Paper 8 at

14 (Oct. 25, 2012) (“we address only the basis, rationale, and reasoning put forth by the [p]etitioner and resolve all vagueness and ambiguity in [p]etitioner’s arguments against the [p]etitioner”); *Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.*, IPR2021-01280, Paper 8 at 22 (PTAB Mar. 9, 2022) (finding petitioner had not met its burden and declining to institute because petitioner’s argument lacked explanation and the Board was unwilling to speculate).

As discussed below, Petitioner presents a convoluted web of alternative “mappings” for claim 1 and generalizations about the prior art. This results in ambiguity regarding how or why, according to Petitioner, a POSITA would have modified Rockwood’s approach to identifying the human behind a computer attack to incorporate Xie’s discussion of anomalous file updates and network forensics. Petitioner structures its petition by discussing claim 1 of the ’045 patent and then incorporating significant portions of that discussion into its arguments regarding the other independent claims (claims 8 and 16). (Petition 44-45, 54-56.) Therefore, deficiencies in Petitioner’s discussion of claim 1 permeate the entire petition.

In connection with claim 1, Petitioner identifies two separate “mappings” of Rockwood for the limitation “gathering one or more events defining an action of a first object acting on a target.” (Petition 14-16.) In the first mapping, the “first object” is a network layer or operating system. In the second mapping, the “first

object” is a data package. Because the “first object” also appears in each of the following three limitations (i.e., “generating a contextual state...,” “obtaining a global perspective...,” and “assembling an event line...”), Petitioner’s alternative mappings of the “first object” also must be addressed in each of those limitations. But the petition does not cohesively address how each mapping would independently render claim 1 obvious. Instead, the petition oscillates between the two mappings in each of the subsequent limitations and at times combines the two.

For example, in its discussion of the “generating a contextual state...” limitation, Petitioner states the following:

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

Petitioner repeats this pattern of purporting to identify the same element in both Rockwood and Xie (and across multiple mappings) without clearly articulating a

specific combination. The Board has rejected “[t]his ‘pick-and-choose’ presentation of evidence,” which “is challenging to follow and makes it difficult to piece together in order to understand Petitioner’s proposed combination or modification.” *Lyft, Inc. v. Quartz Auto Techs., LLC*, IPR2020-01450, Paper 7 at 17-20 (Mar. 4, 2021).

Petitioner also fails to account for the two different applications discussed in Xie, i.e., anomaly detection and network forensics. As addressed above, anomaly detection evaluates file changes within a given computer, and network forensics focuses on identifying the host device (e.g., computer) through which an attack entered the network. (Ex. 1005 at Abstract, 24-25.) Xie discusses anomaly detection in Chapter 2 (Ex. 1005 29-58) and network forensics in Chapter 3 (Ex. 1005 59-120.) Petitioner cherry-picks aspects of each application and applies them interchangeably without any explanation of the context in which they appear in Xie. For example, in discussing motivation to combine, Petitioner cites both the anomaly detection and network forensics applications of Xie interchangeably. (See Petition 12-13; *see also id.* at 20.) Again, the Board has held that this sort of generic application of a reference is not sufficient to identify a combination with specificity. *Lyft*, IPR2020-01450, Paper 7 at 17-20.

And, finally, Petitioner relies extensively on ambiguous and misleading parentheticals to articulate where the prior art purportedly discloses the limitations of the claims. For example, Petitioner states:

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

(Petition 17.) Not only is this contention grammatically confusing, it also appears to suggest that Rockwood discloses identifying the “originating malware” as contextual state information. But, as addressed above, Petitioner’s expert has repeatedly acknowledged that Rockwood is directed to identifying *human* attackers associated with detected suspicious events, not “originating malware.” (EX-1002 ¶¶121, 125, 175, 176.)

Patent Owner and the Board are not required to wade through an ambiguous and convoluted petition to decipher Petitioner’s arguments. *See Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01153, Paper 10 at 16-17 (Jan. 24, 2022) (citing *DeSilva v. DiLeonardi*, 181 F.3d 865, 867 (7th Cir. 1999) (“[a] brief must

make all arguments accessible to the judges, rather than ask them to play archaeologist with the record”) and *United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991) (“Judges are not like pigs, hunting for truffles buried in briefs.”). Because Petitioner fails to articulate its combination with sufficient specificity, the Board should deny institution.

B. Petitioner Fails To Establish That Rockwood In View Of Xie Renders Obvious Claims 1–19

Petitioner’s arguments based on the combination of Rockwood in view of Xie are unlikely to succeed for at least the following reasons.⁷

(1) Petitioner presents two alternative arguments for limitation 1[b], “*gathering one or more events defining an action of a first object acting on a target,*” and similar limitations 8[g] and 16[g]. First, Petitioner argues that the operating system or network layer discussed in Rockwood corresponds to the claimed “first object acting on a target.” But an operating system or network layer is not consistent with the plain and ordinary meaning of an “object” or the “object” claimed in the ’045 patent. Second, Petitioner argues that Rockwood’s data/code package

⁷ As this is a preliminary response, Patent Owner does not address every limitation of every claim. However, this in no way indicates that other limitations and claims are disclosed or rendered obvious by the prior art; indeed, they are not.

corresponds to the “first object acting on a target.” But Rockwood’s data/code package is a packet intercepted during transmission, and thus does not indicate whether it subsequently acts on its target.

(2) Rockwood in view of Xie does not disclose or render obvious claim limitation 1[c], “*generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object,*” or similar limitations 8[h] and 16[h]. Neither Rockwood nor Xie teaches collecting the claimed contextual state information about *originating objects*.

(3) Rockwood in view of Xie does not disclose or render obvious claim limitation 1[d], “*obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object...*,” or similar limitations 8[i] and 16[i]. First, Rockwood’s “global view” is of the entire *system*, not of a particular monitored *event*. Second, Petitioner’s alleged global perspective based on Rockwood/Xie does not include information about related events to the monitored event.

(4) Rockwood in view of Xie does not disclose or render obvious claim limitation 1[e], “*assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object,*

the action of the first object, the target, and the originating object,” or similar limitations 8[j] and 16[i]. Neither Rockwood nor Xie teach an event line that includes the fields of information required by the claims.

(5) A POSITA would not have been motivated to combine Rockwood and Xie because both references embody the prior art problems identified by the '045 patent.

Accordingly, the petition should be denied.

1. Rockwood Does Not Disclose Or Render Obvious Gathering Information About Events Defining An Action Of A First Object Acting On A Target

Claim limitations 1[b], 8[g], and 16[g] each recite gathering an event defining an action of a first object acting on a target. (EX-1001, cls. 1, 8, 16.)

Claim Limitation	Claim Language
1[b]	<i>“gathering one or more events defining an action of a first object acting on a target”</i>
8[g]	<i>“gather one or more events defining an action of a first object acting on a target”</i>
16[g]	<i>“gather one or more events defining an action of a first object acting on a target”</i>

Petitioner relies only on Rockwood for this limitation. (See Petition 14-16, 44, 54.) Petitioner offers two alternative arguments regarding how Rockwood may

disclose the “first object” claim term—that a “first object” may be either (1) the operating system/network layer or (2) a “data/code package.” The Board should reject both arguments.⁸

a) The “Network Layer/OS” Is Not A “First Object”

Petitioner incorrectly asserts a “first mapping” where Rockwood’s operating system/network layer corresponds to the claimed “first object.” (*See, e.g.,* Petition 14 (“the network layer / its operating system (OS) (corresponding to ‘first object’)”), 15-16 (“the network layer / OS (‘first object’) executes on a device”).) On the contrary, a POSITA would not understand a computer’s network layer or operating system to be the “*first object*” recited by the claims of the ’045 patent. (EX-2001 ¶¶63-66.)

First, the claims of the ’045 patent describe the “first object” as an object that is “originated” by another object. (*See* EX-1001 cls. 1[c], 8[h], 16[h].) Specifically, the ’045 patent requires determining an “*originating object of the first object*” in

⁸ Petitioner asserts the same prior art references (Rockwood and Xie) against the same claim language in U.S. Patent 10,257,244, which issued as a continuation of the ’045 patent. *See* Case IPR 2023-00657, Paper 6. Both petitions fail for the same reasons.

order to generate contextual state information. (See EX-1001 claim 1[c].) See also Section III, *supra*. Petitioner does not identify any disclosure in Rockwood (or anywhere else) that discloses or explains how an operating system or network layer is originated by another object. (See EX-2001 ¶¶63-66.)

Petitioner asserts that Rockwood's "source[] of attack[] or originating malware" is the claimed "originating object." (Petition 17-18 ("A PHOSITA would have recognized that the sources of attacks or originating malware (corresponding to 'originating object of the first object') corresponding to detected events would be generating events/attacks to be transmitted via the network layer/OS ('first object')."). But under Petitioner's theory, to comport with the '045 claims, the "source[] of attack[] or originating malware" would have to *originate* a computer's network layer or operating system, which is unsupported and nonsensical. Malware is not the originating object of a network layer or operating system. (EX-2001 ¶¶64–66.) As Petitioner's expert Dr. Nielson acknowledges, malware is "harmful application software (e.g., a process) that generates unwanted network traffic and causes the network layer to transmit it." (EX-1002 ¶166; see also ¶72 ("'Malware' ... causes harmful (or unauthorized at the very least) operations to a victim's computing systems.').) A POSITA would *not* understand Rockwood as disclosing a

computer network layer or operating system that originates from “unwanted network traffic” or “harmful application software.” (EX-2001 ¶¶64-66.)

Second, claims 1 and 8 recite a “global perspective” that may include “a determination as to whether the first object is malware.” (EX-1001 cls. 1, 8). A POSITA would understand that an operating system and a network layer would never be considered “malware” at least because they are not “harmful application software” that “generates unwanted network traffic.” (EX-2001 ¶¶67.)

Third, the '045 patent's description of “computer objects” as “a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated, or interpreted” is inconsistent with Petitioner's argument that an operating system or network layer can be the claimed “first object.” (EX-1001 7:31-54; EX-2001 ¶¶68.) A POSITA would understand network layers and operating systems generally as software implemented by robust packages of interrelated and interdependent files, whereas the '045 patent describes computer objects as computer files or similar objects that are discrete and far smaller than a computer's operating system or network layer. (EX-2001 ¶¶68.)

Thus, Petitioner's argument that Rockwood's network layer and/or operating system discloses the claimed "first object" is wrong and should be rejected. (EX-2001 ¶¶64-69.)

b) Rockwood's "Data/Code Package" Does Not Disclose Or Render Obvious An "Event Defining An Action Of A First Object Acting On A Target"

Petitioner's "second mapping" identifies a data/code package as the claimed first object. (Petition 16 "In a second mapping, Rockwood also discloses ... the data/code package (corresponding to 'first object') is transmitted..."; Rockwood notes that the data package includes executable code (corresponding to 'first object')..."). Petitioner's second mapping fails to identify any disclosure or teaching of an "event defining an action of a first object acting on a target."

First, Petitioner's second mapping is based on the erroneous suggestion that malware being transmitted can be both the originating object and the first object. As discussed below, that cannot be the case. *See* Section V.B.2, *infra*, discussing limitation 1[c]. If originating malware is the originating object as Petitioner asserts, then there is no "first object" of an event defining an action of a first object acting on a target.

Second, Rockwood does not disclose any computer object that is "acting" on a target. The '045 patent describes the claimed "action" on a target as an event type,

such as a registry edit, that has been performed on a target. (EX-1001 17:20-29.) By contrast, Petitioner's claim that Rockwood discloses transmitting a data package that "may be malware" does not define a first object "acting" on a target. Petitioner identifies the alleged target as a destination IP address. (Petition 16 *see above*.) But Petitioner does not identify, and Rockwood does not disclose, "*an action*" of the data/code package at that target IP address. Transmitting the data that may be malware is not an action that is performed on the destination IP address (Petitioner's "target"). (EX-2001 ¶¶71-73.)

Indeed, Rockwood indicates that the data/code is intercepted during transmission. Rockwood describes collecting event information from a transmitted packet's headers to determine the packet's source and intended destination, and the packet payload to identify the packet's contents. (EX-1004 3:36-55; *see also id.* at 5:51-53 ("Then, upon receiving a request from the operator, GUI 52 expands the visual representation of event information *to display packet headers and payloads to the operator.*") (emphasis added).) A packet, or data/code package, that has been intercepted en route to its destination *does not* indicate whether it was ever subsequently received by its intended destination, and certainly cannot indicate whether its contents (i.e., the data/code package petitioner maps as the first object) takes any action on an intended target. (EX-2001 ¶71.)

The two Rockwood excerpts Petitioner cites do not describe an object *acting* on a target either. (EX-2001 ¶¶71-73.) Petitioner's first cite (3:50-60) describes operation of Rockwell's network edge sensors, which "may use algorithms, signatures, scripts, or any suitable detection or comparison technique to process packet headers, packet payloads, and/or any other data." (Petition 16 (citing EX-1004 3:50-60).) This information about Rockwell's sensors, and the fact that they communicate detected events, does not disclose or render obvious an event based on "an *action of a first object acting on a target*." Instead, the alleged "first object" (the "data/code package") is simply being *transmitted* from the source of an event to a destination IP address—it is not *acting on* anything. (EX-2001 ¶¶71-73.)

Petitioner's second cite describes detecting an "enemy hacker" attempting to hack into the system. (Petition 16 (citing EX-1004 12:35-45 ("In the present example, an enemy attacker attempts to hack into system 10 to obtain sensitive information about supply levels tracked by system 10. System 10 detects this attack as detected event 110f, which occurred at 5:20 p.m. and originated from a UNIX-based computer. Detected event 110f contains a segment of code signifying that detected event 110f is an attack.")) While this disclosure describes detection of an attempted attack and identifies the source of the attack (a UNIX-based computer), none of this information describes a particular computer object acting on the

destination IP address (Petitioner's "target"). (EX-2001 ¶73.) Simply put, even if a POSITA could understand Rockwood's described attack information as an event based on the transmission of a computer object, it does not disclose or teach that the event involves a first object acting on a target.

To the extent Petitioner suggests that Rockwood's disclosure of detecting attack events somehow implies that a computer object must have acted on a destination IP address, it is incorrect and contrary to Rockwood's teachings. Rockwood defines an "attack" without regard to whether a computer object acts on a target. (EX-1004 2:65-3:4 ("An 'attack' may be any malicious, destructive, or suspicious activity *communicated from a source external and/or internal to the portion of the enterprise protected by system 10*. Attacks may include viruses, Trojan horses, worms, or any other piece of code or data that represents at least a portion of *an unwanted attempt to access the protected portion of the enterprise*.")) (emphasis added).) In other words, Rockwood's "attack" describes communicating (transmitting) malicious activity and unwanted attempts to access the protected portion of an enterprise. Rockwood's references to an "attack" do not disclose an event that involves (i) transmission of a specific malicious computer object to a destination IP address (Petitioner's "target"), and (ii) an effect/action of that malicious computer object on that destination IP address. (EX-2001 ¶74.)

Therefore, under both of Petitioner's theories for the "first object" limitation, Rockwood fails to disclose or render obvious at least claim limitations 1[b], 8[g], and 16[g], which all require "*gather[ing] an event defining an action of a first object acting on a target.*"

2. The Rockwood/Xie Combination Does Not Disclose Or Render Obvious "Generating A Contextual State..." That Includes The Claimed "Originating Object"

Claim limitations 1[c], 8[h], and 16[h] each require generating contextual state information for an event by correlating the event to an originating object of the first object. (EX-1001, cls. 1, 8, 16.)

Claim Limitation	Claim Language
1[c]	<i>"generating a contextual state for at least one of the one or more events by correlating the at least one event to an <u>originating object</u>, the contextual state including an indication of the <u>originating object of the first object</u> and an indication of at least one of a device on which the first object is executed and a user associated with the first object;"</i>
8[h]	<i>"generate a contextual state for at least one of the one or more events by correlating the at least one event to an</i>

Claim Limitation	Claim Language
	<i><u>originating object</u>, the contextual state including an indication of the <u>originating object of the first object</u> and an indication of at least one of a device on which the first object is executed and a user associated with the first object”</i>
16[h]	<i>“generate a contextual state for at least one of the one or more events by correlating the at least one event to an <u>originating object</u>, the contextual state including an indication of the <u>originating object of the first object</u> and an indication of at least one of a device on which the first object is executed and a user associated with the first object”</i>

As the '045 patent explains, an “originating object” is an object that initiates or otherwise creates the first object. (EX-1001 17:39-42 (“[T]he originating process or object may be determined based on a previous event that initiated or otherwise created the current process and/or object.”).) Correlating events to their originating objects allows administrators to follow an audit trail “to forensically track back any event which occurs to what triggered it.” (Ex-1001 3:45-49.) Petitioner fails to

identify any disclosure or suggestion of the claimed “originating object” in either Rockwood or Xie. (EX-2001 ¶¶78–84.)

Petitioner's arguments regarding this limitation are among the most convoluted in the petition. For example, the following sentence appears in the first paragraph of Petitioner's argument:

Rockwood and Xie disclose using an attacker profile to correlate an event to an originating object/process of the first object (e.g., originating malware or source) of an attack that causes a network layer / OS (‘first object’) to transmit data such as an attack/malware (e.g., copy of the originating malware)), wherein such correlated data (corresponding to ‘contextual state’) includes information such as originating processes/objects, devices, and users (as discussed below).

EX1002, ¶¶166-170; EX1004, 2:60-3:5,6:1-62,13:1-24.

How that articulates the purported disclosure of limitation 1[c] in the prior art is anyone's guess. But the reason Petitioner finds itself twisted in knots around this limitation is clear: neither Rockwood nor Xie has anything to do with identifying an object that initiates or otherwise creates another object (e.g., the first object). Rockwood is directed to identifying a human attacker. Xie is directed to identifying anomalies associated with file updates and the *computer* (not the object) that

originated an attack. To the extent Petitioner's arguments regarding this limitation are discernable, they are wrong for the reasons addressed herein.

a) Rockwood Does Not Disclose Or Render Obvious The Claimed "Originating Object"

As discussed above, the claims recite an "originating object" that initiates or otherwise creates a "first object" and require "correlating the at least one event to an originating object."

Petitioner's "first mapping" assumes that a network layer/operating system in Rockwood is the "first object." However, Petitioner does not identify any object that initiates or otherwise creates the network layer/operating system. Petitioner appears to suggest that the "attacker profile or originating malware" is the "originating object." (Petition 17 ("attacker profile or originating malware ('originating object')").) However, Rockwood's attacker profile is simply a data structure with a collection of information about a *human* attacker. (See EX-1002 ¶¶121, 125, 175, 176.) There is no disclosure in Rockwood that an attacker profile is itself a computer object or that it initiates or otherwise creates a network layer or operating system. (EX-2001 ¶¶78-80.)

Petitioner's argument regarding "originating malware" fares no better. Rockwood does not use the term "originating malware," which Petitioner appears to have created out of whole cloth. Nor does Rockwood explain (i) how malware would

initiate or otherwise create a network layer or operating system (EX-2001 ¶¶78-80) or (ii) how an event would be correlated to malware. Rockwood unremarkably notes that “[a]ttacks may include viruses, Trojan horses, worms, or any other piece of code or data that represents at least a portion of an unwanted attempt to access the protected portion of the enterprise.” (EX-1004 3:1-4.) Petitioner appears to bootstrap this into its “originating malware” argument based on nothing more than an unsupported expert declaration. (Petition 17-18, citing EX-1002 ¶¶166-171.) But Rockwood does not address identifying the *objects* that originate such attacks or correlating events to those objects. Again, Rockwood is directed to identifying the *human* behind an attack. (EX-2001 ¶¶ 44, 78-80; EX-1002 ¶¶121, 125, 175, 176.)

Petitioner’s “second mapping” similarly fails to identify where the claimed “originating object” is taught by Rockwood. Although Petitioner previously identified a data/code package as the “first object” in connection with this limitation, Petitioner characterizes the “first object” as “transmitted malware” and again suggests that certain unspecified “originating malware” is the “originating object.” (Petition 19.)⁹ In other words, Petitioner appears to identify the same malware as

⁹ Another confounding characteristic of the petition is its loose and inconsistent verbiage when articulating whether prior art purportedly discloses certain

both the first object and the originating object. Again, none of Petitioner's arguments are based on any disclosure actually found in Rockwood. As addressed above, Rockwood does not use the term "originating malware," and it does not explain (i) how malware would initiate or otherwise create malware or (ii) how an event would be correlated to malware. Rather, Petitioner's argument is based solely on an unsupported expert declaration untethered to Rockwood's disclosure. (Petition 19, citing EX-1002 ¶¶171-173.)

**b) Xie Does Not Disclose Or Render Obvious The
Claimed "Originating Object"**

Petitioner argues that Xie discloses an "originating object." (Petition 18-19.) As addressed above, Petitioner argues that Rockwood also discloses this limitation.

limitations. For example, just in connection with the "originating object" claim term, the petition variously refers to: "an originating object/process of the first object (e.g., originating malware or source) of an attack," "an attacker profile or originating malware ('originating object')," "sources of attacks or originating malware (corresponding to 'originating object of the first object')," "originating malware of an attack ('originating object')," "source of attack/originating object is the originating malware ('originating object')," and "source behind an attack / attacker profile (e.g., originating malware/object)."

Although Petitioner appears to contend that Xie should be combined with Rockwood, the petition does not clearly identify what element is missing from Rockwood that is allegedly disclosed in Xie. *See Lyft*, IPR2020-01450, Paper 7 at 18 (denying institution where petitioner “[did] not articulate adequately how it propose[d] to modify one of the references or to combine the two references’ teachings”).

Regardless, Petitioner first argues that “Xie discloses identifying the identity/name and location of the originating malware (e.g., Lion worm) based on correlations of network events and file events on the network (e.g., file changes in network devices that indicate presence of an attack and its source (originating malware)).” (Petition 18.) That is not correct. Xie does not “identify” the name and location of originating malware at all, much less by using “correlations” of network events and file events on the network. Xie’s authors selected the Lion worm as the exemplary piece of malware to test the Seurat prototype. (EX-1005 47 (“[W]e ***limit our attention to one worm for illustrative purposes*** and present the result with the Lion worm in this experiment.”) (emphasis added).) Xie’s Seurat system did not identify the Lion worm among other possible computer objects. (*See* EX-2001 ¶¶82-84.) The worm was known from the outset. (*Id.*)

Moreover, Petitioner does not identify any disclosure from Xie (or Rockwood) about identifying, analyzing, or attempting to determine how computer objects may be related to other computer objects. (See EX-2001 ¶¶81-84; see generally Petition 17-21.) Xie's file change monitoring does *not* disclose any attempt to compare different objects to determine whether computer objects are related. Thus, even if Xie could be described as identifying potentially suspicious files based on file system changes, it still does not analyze or determine relationships between computer objects that would constitute a contextual state that includes an indication of an *originating object of a first object*, as required by the challenged claims. (See EX-2001 ¶¶81-84.)

Petitioner argues that Xie uses “broader event data” to “more clearly identify the files associated with malware on a device (e.g., originating malware that is the source of an attack)” (Petition 12.) Petitioner cites the network forensics application addressed in Xie, and not the anomalous file update application. However, Petitioner offers no explanation for how the different applications in Xie would be combined with Rockwood. In its network forensics application, Xie discloses identifying infected “host” devices (e.g., computers). (EX-1005 61-65; EX-2001 ¶¶82-84.) A host device is not an originating *object*—it is not an object at all. (EX-1001 7:32 – 36 (“An object in this sense may be a computer file, part of a file or a sub-program,

macro, web page, or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted.”.) *See also* Section V.A., *supra*.

Petitioner further argues that “Xie teaches identifying originating malware of an attack (‘originating object’) (e.g., that causes a network layer / OS (‘first object’) to transmit malware), based on correlated events and connecting those events to the code and affected files constituting the malware within the OS (e.g., Linux/Windows) and its source (originating malware).” (Petition 18 (citing EX-1005 30-32, 47-49); EX-1002, ¶¶179-181.) Based on the reference to the “network layer / OS,” Petitioner appears to associate this argument with its “first mapping” of Rockwood. But as discussed above, the “originating malware” that Petitioner identifies cannot be the “originating object” because the originating object creates or initiates the first object, and the malware Petitioner points to in Xie does not originate the “network layer / OS” that Petitioner identifies as Xie’s first object.

Petitioner does not appear to present a different argument regarding Xie in connection with its “second mapping” of Rockwood. (Petition 19 (“Rockwood and Xie disclose this limitation for the same reasons above.”).) However, Petitioner appears to conflate its arguments regarding its two mappings of Rockwood and Xie. Petitioner states: “Under either mapping, Rockwood and Xie disclose associating an

event (containing the data package ('first object' under the second mapping)) with a source behind an attack / attacker profile (e.g., originating malware/object) that caused a network layer/OS ('first object' under the first mapping) to transmit the data, to generate contextual state and thus disclose 'the contextual state including an indication of the originating object of the first object.' EX-1002 ¶¶170-173,187-190; EX-1004, 6:25-35,7:20-25,8:6-65,13:1-25,15:65-16:7." (Petition 20.) As addressed above, this conclusory statement does not clearly articulate a specific combination of prior art teachings. *See* Section V.A., *supra*.

Accordingly, Petitioner fails to establish a reasonable likelihood of success to show limitations 1[c], 8[h], and 16[h] are disclosed or rendered obvious by Rockwood in view of Xie.

3. The Rockwood/Xie Combination Does Not Disclose Or Render Obvious The Claimed "Global Perspective" For A Recited Event That Includes Related Events Across A Network

Claim limitations 1[d], 8[i], and 16[i] each require global perspective information comprising information about one or more related events to the one or more events across a network. (EX-1001 cls. 1, 8, 16.)

Claim Limitation	Claim Language
1[d]	"obtaining a global perspective for the at least one event .

Claim Limitation	Claim Language
	<i>. . wherein the global perspective for one or more related events to the at least one event across a network;”</i>
8[i]	<i>“obtain a global perspective for the at least one event ... wherein the global perspective for one or more related events to the at least one event across a network;”</i>
16[i]	<i>“global perspective information comprising information about one or more related events to the one or more events across a network;”</i>

Petitioner incorrectly asserts that Rockwood’s “global view” is the “global perspective” recited by the claims. (Petition 21-22, *see also* 23-25.) All challenged claims explicitly require a “global perspective” that is specific to an event. (*See, e.g.,* EX-1001 cls. 16[i] (“global perspective information comprising information ***about one or more related events to the one or more events across a network***”) (emphasis added); 1[d], 8[i] (“wherein the global perspective for ***one or more related events to the at least one event across a network.***”) (emphasis added).) Indeed, the district court’s claim construction for “global perspective” included clarifying language to

confirm that its “plain-and-ordinary meaning is ‘information about *events related to the monitored even[t] across a network.*’” (EX-2010 8 (emphasis added).)¹⁰

Contrary to Petitioner's argument, Rockwood does not disclose or suggest obtaining the event-specific “global perspective” recited in the challenged claims. Petitioner wrongly asserts that “Rockwood discloses correlating the event to other events and attributes across the network to generate a global view of an attack using attacker profiles (as modified by Xie) (corresponding to ‘obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object’).” (Petition 21.) But the only “global view” Rockwell discloses is for the *state of a computer system*, not a particular monitored *event* as claimed. (EX-2001 ¶¶87-89; EX-1004 14:24-29 (“Global server 40 then processes detected events 110 and provides operator 60 with a *global view of the state of system 10*”) (emphasis added); 19:27-31 (“According

¹⁰ Petitioner asserts the same prior art references (Rockwood and Xie) against U.S. Patent No. 10,257,244, which issued as a continuation of the '045 patent. *See* Case IPR 2023-00657, Paper 6. The '224 patent includes substantially identical claim language to the “global perspective” claim language in the '045 patent. Both petitions fail for the same reasons.

to certain embodiments GUI 52p in network node 610p displays n-dimensional graphs 340p, 340q, 340r, and 340s to operator 60p of network node 610p. Thus, operator 60p obtains a *more complete view of the state of system 10.*") (emphasis added).) Rockwood does not disclose how the global view is obtained, what information is used in obtaining the global view, or what state of the system information it includes. (EX-1004 14:29; EX-2001 ¶¶87-89.). Petitioner fails to explain how a POSITA would transform Rockwood's general view of the overall state of a computer system, even if modified by Xie in some unknown manner, into the particular claimed global perspective for an event that includes information about related events across a network.

Petitioner fares no better with its conclusory argument that "a POSITA would have understood that the network-level aggregation and global view of events across a network (comprising multiple devices) in Rockwood based on the correlated data as modified by Xie teach obtaining the recited global perspective." (Petition 24.) This argument fails for the same reasons stated above: it fails to explain how Rockwood's network-level aggregation discloses or renders obvious obtaining a "global perspective" of a particular monitored *event* in relation to other events across a network. A general network-level aggregation of all detected events does not equate to obtaining a global perspective for a particular event that includes

identifying information about related events across the network. (*See, e.g.,* EX-1001 cl. 16[i] (“information about one or more ***related*** events to the one or more events ***across a network.***”); EX-2001 ¶¶88-90 (emphasis added).) Petitioner does not explain how Rockwood’s aggregated information might represent a particular monitored event or how such an event may be determined to be related to other events across a network. (*See* Petition 21-26.) Petitioner also fails to articulate exactly how Xie’s localized Lion worm testing somehow transforms Rockwood’s network aggregation into the claimed “global perspective.” (EX-2001 ¶¶89-91.)

Petitioner’s assertions concerning this claim limitation and how Xie allegedly rewrites Rockwood’s network-level aggregation as the claimed “global perspective” are vague and conclusory and should be rejected. *See T-Mobile US, Inc. v. TracBeam LLC*, IPR2015-01687, Paper 10 at 20 (PTAB Feb. 12, 2016) (“We will not, however, piece together evidence in an attempt to establish a ground or improperly shift the burden of deciphering the arguments onto the Patent Owner or ourselves.”); *Billy Goat Indus., Inc. v. Schiller Grounds Care, Inc.*, Case IPR2014-00742, Paper 8 at 28 n.4 (PTAB Nov. 7, 2014) (“It is Petitioner’s responsibility to explain specific evidence that support its arguments, not the Board's responsibility to search the record and piece together what may support Petitioner's arguments.”).

As a result, Petitioner fails to establish that Rockwood and Xie disclose or render obvious the claimed global perspective for a monitored event that is based on information about an originating object and a first object, and includes information about one or more related *events* across a network.

**4. The Rockwood/Xie Combination Does Not Disclose Or
Render Obvious The Claimed Event Line**

Claim limitations 1[e], 8[j], and 16[i] each require generating an event line comprising information relating to the event, wherein the information includes the first object, the action of the first object, the target, and the originating object. (EX-1001, cls. 1, 8, 16.) Petitioner's combination does not disclose or render obvious this limitation.

Claim Limitation	Claim Language
1[e]	<i>“assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object;</i>
8[j]	<i>“assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of</i>

Claim Limitation	Claim Language
	<i>the first object, the target, and the originating object;</i> "
16[i]	<i>"assemble an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network"</i>

Petitioner fails to identify any teaching from Rockwood or Xie of an “*event line*” that includes the claimed details associated with the event, such as information uniquely identifying the first object, the action of the first object, the target, and the originating object, and global perspective information about one or more related events across a network. (EX-2001 ¶¶95-98.)

Petitioner argues that Rockwood’s display of an attacker profile, as modified by Xie, on a graphical user interface discloses or renders obvious the claimed “*event line*” limitation. (Petition 26–28.) But Rockwood’s modified attacker profile does not include the event line information that the claims require, i.e., information uniquely identifying the first object, the action of the first object, the target, and the

originating object. (EX-1001 cls. 1[e], 8[j], 16[i]; EX-2001 ¶95; *see* Petition 26 (citing EX-1004 5:48-51, 7:3-10, 7:20-22, 10:34-44, 16:62-66).)

For example, Petitioner fails to identify an event line that includes details of an originating object. Petitioner points to the “attacker profile” as the “originating object” for this claim limitation. (Petition 26 (“For example, Rockwood discloses displaying the attacker profile (‘originating object’) on the GUI in connection...”).) As discussed above, the attacker profile is not an originating object. *See* Section V.B.2, *supra*. Thus, any information about the “attacker profile” would not include detailed information about the “originating object” as the event line claim recites.

Petitioner's further reliance on Rockwood / Xie and the “reasons discussed” in the petition “regarding limitations 1[b] and 1[c]” likewise fails to disclose the claimed event line information identifying an “originating object.” (Petition 27.) As discussed above, Petitioner identifies “originating malware” as the “originating object” in both mappings. (Petition 17.) But originating malware cannot be in Rockwood or Xie cannot be the claimed originating object. *See* Section V.B.2, *supra*. In addition, the Rockwood/Xie combination fails to disclose a “global perspective” that includes information about events related to a particular event across a network. *See* Section V.B.3, *supra*

Accordingly, Petitioner fails to identify anything in Rockwood, Xie, or their combination that a POSITA would understand to be an event line that includes detailed information about at least the “originating object” or the “global perspective” as claimed. (EX-2001 ¶¶ 95-98.) Petitioner fails to meet its burden on institution. *Harmonic*, 815 F.3d at 1363; *Lumenis*, IPR2021-01280, Paper 8 at 22.

5. A POSITA Would Not Have Been Motivated To Combine Rockwood With Xie Because Each Reference Embodies The Problems Of The Prior Art

A POSITA would not have been motivated to combine Rockwood and Xie because neither reference teaches collecting contextual information regarding an observed event from within the host or system that generates the event. *See* Section IV, *supra*. (EX-2001 ¶¶100-102.) As discussed above, both Rockwood and Xie perform their respective network forensic analysis techniques using sensors placed along communication pathways so that the sensors collect transmitted network traffic. *See* Section IV, *supra*. This aspect of the prior art is precisely the problem the '045 patent sought to address. (*See* EX-1001 1:36–51.) As explained by the '045 patent's written description:

[E]xisting network forensics tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events

outside of a host or system. That is, a network forensic tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or more hosts or systems. Accordingly, network edge devices have no ability to establish any sort of context from within the host or system that is generating the event. Therefore, devices residing at a network edge may monitor, record, and or analyzes network traffic between the host and the device, but information that may be useful within the host is not obtained.

(See EX-1001 1:36–51.) Neither Rockwood nor Xie collects information about an event *from* host computers; each instead relies on intercepting network transmissions *outside* host computers using sensors along the network's communications pathways. See Section IV.A-B *supra*. (EX-2001 ¶¶100-102.)

As also discussed above, the Rockwood/Xie combination fails to identify or collect the recited information about the “originating object” because it does not obtain information about *computer objects*’ actions from a host computer. See Section V.A.2, *supra*. (EX-2001 ¶102.) Rather, Petitioner relies on disclosures from Rockwood related to an attacker profile that identifies an *individual* attacker (Petition 17-18) and disclosures from Xie that identify the *source node/computer* of an attack. (Petition 20 citing EX-1005 61, 63.) Accordingly, POSITA would not have been motivated to combine Rockwood and Xie for the *originating object* limitation because neither reference teaches collecting information about which computer objects may have originated other computer objects.

Given the stark differences between these references and the claimed invention—particularly in view of the '045 patent's instruction that network edge devices do not provide useful contextual information from within a monitored device about events—a POSITA would not have been motivated to combine Rockwood with Xie, which each suffer from the deficiencies identified by the '045 patent, to practice the claims of the '045 patent.

C. Petitioner's Grounds Fail To Anticipate Or Render Obvious All Dependent Claims

Because Petitioner has failed to establish that any of its grounds anticipate or render obvious all limitations of independent claims 1, 8, and 16, Petitioner cannot make a showing that such grounds anticipate or render obvious dependent claims 2–7, 9–15, and 17–19.

D. Secondary Objective Indicia Of Nonobviousness

Patent Owner contends that secondary indicia of nonobviousness exist and reserves its right to provide evidence on this point, should the Board institute. (EX-2001 ¶¶106–109.)

VI. CONCLUSION

For the foregoing reasons, the challenged claims of the '045 patent are patentable and the Board should decline to institute IPR.

Patent Owner's Preliminary Response
to Petition for *Inter Partes* Review
Patent No. 9,578,045

Date: August 10, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /s/ Brian Eutermoser

Brian Eutermoser

Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 have 13,822 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word 365 V.2202.

Date: August 10, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /s/ Brian Eutermoser

Brian Eutermoser

Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2019** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) and sent via electronic mail in their entireties on the following:

Robert M. Hansen (Reg. No. 43,656)
Scott B. Amankwatia (Reg. No. 78,226)
Matthew J. Anderson (Reg. No. 78,257)
THE MARBURY LAW GROUP, PLLC
11800 Sunrise Valley Drive, 15th Floor
Reston, Virginia 20191
Email: rhansen@marburylaw.com;
Email: samankwatia@marburylaw.com
Email: manderson@marburylaw.com
Email: pat-docketing@marburylaw.com

Date: August 10, 2023

KING & SPALDING LLP

BY: /s/ Brian Eutermoser

Brian Eutermoser

Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.