

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

**DECLARATION OF PROFESSOR NENAD MEDVIDOVIC, Ph.D.
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE**

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

TABLE OF CONTENTS

I.	QUALIFICATIONS	2
II.	UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	7
III.	STATE OF THE PRIOR ART	10
IV.	THE '045 PATENT	12
	A. Summary of the '045 Patent.....	12
	B. Claim Construction	15
	C. Level Of Ordinary Skill In The Art.....	17
V.	OVERVIEW OF PRIOR ART	19
	A. Overview of Rockwood (EX-1004)	19
	B. Overview of Xie (EX-1005).....	25
	1. Anomaly Detection Using Spatiotemporal Correlation.....	25
	2. Network forensics using spatiotemporal event correlation	27
VI.	ROCKWOOD IN VIEW OF XIE DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS.....	28
	A. Rockwood's Does Not Gather Information about Objects Acting on Targets or Executing on Devices	31
	1. The "Network Layer/OS" Is Not a "First Object"	31
	2. Rockwood Does Not Disclose or Render Obvious an Event Defining a First Object Acting on a Target	34
	B. The Rockwood-Xie Combination Does not Disclose or Render Obvious the "Originating Object"	39
	1. Rockwood Does Not Disclose or Render Obvious the Claimed "Contextual State" and "Originating Object"	40

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

2.	Xie Does Not Teach the Claimed “Contextual State” and “Originating Object”	42
C.	Rockwood Does Not Obtain a Global Perspective for the Event	44
D.	Rockwood / Xie does Not Disclose or Render Obvious the Claimed Event Line.....	49
E.	A POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art	52
F.	Dependent Claims	54
VII.	CLAIMS AND/OR LIMITATIONS NOT ADDRESSED IN THIS DECLARATION	55
VIII.	SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS	55
IX.	CONCLUSION.....	56

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

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

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

Exhibit	Description
	Through 2023, “Table N/A – U.S. District Courts – Combined Civil and Criminal 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)

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

Exhibit	Description
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)
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)

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

I, Professor Nenad Medvidovic, Ph.D., declare as follows:

1. I have been engaged by King & Spalding LLP on behalf of OpenText Inc. ("Patent Owner"), to provide this Declaration concerning the technical subject matter relevant to the petition for *Inter Partes* Review ("Petition") of U.S. Patent 9,578,045 ("the '045 patent").

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have reviewed and am familiar with the specification and the claims of the '045 patent. In general, I will cite to the specification of a United States patent using the following formats: (Exhibit No. Col:Line Number(s)) or (Exhibit No. Paragraph Number(s)). For example, the citation (EX-1001 1:1–10) points to the '045 patent specification at column 1, lines 1–10. Also, for convenience, I use italics to denote limitations from the challenged claims.

4. All the opinions in this Declaration are based on the documents I have reviewed and my knowledge and professional judgement. In forming the opinions expressed in this Declaration, I reviewed the Petition for *Inter Partes* Review of U.S. Patent No. 9,578,045 and supporting exhibits.

5. I have been asked to provide my technical opinions on how concepts in the '045 patent specification relate to claim limitations of the '045 patent. In reaching the opinions provided herein, I have considered the '045 patent, its prosecution history, and the references cited above and have drawn as appropriate on my own education, training, research, knowledge, and personal and professional experience.

II. QUALIFICATIONS

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, experience, and publications is set forth in my *curriculum vitae* (CV), which is submitted as Exhibit 2002.

7. I received a Bachelor of Science degree, *Summa Cum Laude*, from Arizona State University's Computer Science and Engineering department.

8. I received a Master of Science degree from the University of California at Irvine's Information and Computer Science department.

9. I received a Doctor of Philosophy degree from the University of California at Irvine's Information and Computer Science department. My dissertation was entitled "Architecture-Based Specification-Time Software Evolution."

10. For nearly 30 years, my research has focused on the building blocks that comprise software systems: software components (computational and data elements) and connectors (interaction-facilitating elements), and mechanisms for their implementation, primarily middleware facilities and software frameworks. In particular, my Ph.D. dissertation—whose first research results were published in 1995 while the dissertation was completed in 1999—yielded a new design style for the development and evolution of highly distributed software systems built out of independent components that exchange different types of information encoded in messages in order to accomplish specific goals. This research focused on the design principles behind such systems, the appropriate support for modeling the systems (both at the level of individual agents as well as their integrations into subsystems and entire systems), and the infrastructure for their implementation, deployment, and optimization. This work was applied across a wide range of domains, from traditional distributed systems to mobile devices and autonomous robots.

11. I am employed by the University of Southern California (“USC”) as a faculty member in the Computer Science Department and have been since January 1999. I currently hold the title of Professor with tenure. Since July 2022, I have served as my department’s Chairman. Between January 2009 and January 2013, I served as the Director of the Center for Systems and Software Engineering at USC.

Between July 2011 and July 2015, I served as my Department's Associate Chair for Ph.D. Affairs. Between July 2021 and June 2022, I served as my Department's Vice-Chair for Tenure Affairs.

12. I teach graduate and undergraduate courses in Software Architecture, Software Engineering, and Embedded Systems, and I advise Ph.D. students. I have graduated 19 Ph.D. students and advise 10 students currently pursuing a Ph.D.

13. I served as Program Co-Chair for the flagship conference in my field—International Conference on Software Engineering (“ICSE”)—held in May 2011. I have served as Chair or Co-Chair for various other conferences in the Software Engineering field, including: the Fifth Working Institute of Electrical and Electronics Engineers (“IEEE”)/IFIP Conference on Software Architecture, the Third IEEE International Conference on Self-Adaptive and Self-Organizing Systems, the Fifteenth International Association for Computing Machinery’s (“ACM”) Special Interest Group on Software Engineering (“SIGSOFT”) Symposium on Component Based Software Engineering, the IEEE/CSSE/ISE Workshop on Software Architecture Challenges for the 21st Century, and the Doctoral Symposia at the 16th ACM SIGSOFT International Symposium on the Foundations of Software Engineering and at the 44th International Conference on Software Engineering. I am currently serving

as General Co-Chair of the 21st International Conference on Software Architecture (ICSA 2024).

14. I serve or have served as an editor of several peer-reviewed journals, including: “IEEE Transactions on Software Engineering,” “ACM Transactions on Software Engineering and Methodology,” “Journal of Software Engineering for Robotics,” “Elsevier Information and Software Technology Journal,” “Journal of Systems and Software,” “Journal of Software Engineering Research and Development,” and “Springer Computing Journal.” Additionally, I have served as a guest editor of several special issues for different journals. Since January 2018, I have served as Editor-in-Chief of “IEEE Transactions on Software Engineering.”

15. Between September 2013 and September 2015, I served as Chair of the ICSE Steering Committee. Both prior to that (2008-2013) and subsequent to that (2015-present) I have been a member of the ICSE Steering committee. I am currently a member of the Steering Committee of the joint European Conference on Software Engineering and the Symposium on the Foundations of Software Engineering (“ESEC/FSE”). From July 2015 to September 2017, I chaired the Steering Committee of FSE, while it was a standalone symposium. I previously served as a member

of the Steering Committees of the Working IEEE/IFIP Conference on Software Architecture.

16. Between July 2015 and June 2018, I served as Chair of the ACM SIGSOFT, the largest professional organization in my field of work. During the past year, I have chaired the Committee in charge of ACM's Software System Award, one of the most important technical awards given in my field.

17. I co-authored "Software Architecture: Foundations, Theory, and Practice," a widely used textbook in the field of Software Systems' Architecture.

18. I have served as editor of various books in the Software Engineering field including: "Proceedings of the 3rd International Conference on Self-Adaptive and Self-Organizing Systems," "Proceedings of the Warm-Up Workshop for the 32nd International Conference on Software Engineering," "Proceedings of the 5th Working IEEE/IFIP Conference on Software Architecture," and "40 Editions of ICSE – The Ruby Anniversary Celebration."

19. I have authored or co-authored nearly 300 papers in the Software Engineering field. My most cited paper has been cited well over 3,000 times. A paper I co-authored in the 1998 International Conference on Software Engineering, my field's flagship conference, was given ten years later, in 2008, that conference's Most

Influential Paper Award. Another one of my publications received a Most Influential Paper Award in 2020. Several of my other publications have received “best paper” or “most cited” awards.”

20. Several of my publications have focused on different aspects of computer security. A paper describing a security-vulnerability detection tool for Android devices, built in my lab, won the Best Tool Paper award at the 2017 Automated Software Engineering Conference. I have co-authored three patents in the area of cybersecurity.

21. I have been named a Distinguished Scientist of the ACM. I have been elected a Fellow of the IEEE, IEEE's highest grade that is granted to less than 0.1% of its membership annually.

III. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES

22. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

23. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the

requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

24. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called “secondary considerations” of nonobviousness if they are present.

25. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

- 1) Identify the particular references that, singly or in combination, make the patent obvious;
- 2) Specifically identify which elements of the patent claim appear in each of the asserted references; and

3) Explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of known element for another to obtain predictable results;
- Use of known technique(s) to improve similar devices (methods or products) in the same way;
- Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
- “Obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
- Known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predictable to a person of ordinary skill in the art; and

- Some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or to combine the prior art reference teachings to arrive at the claimed invention.

26. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

27. I have been informed that a prior art reference may be relied upon not only for what it expressly teaches, but also for what is inherent therein—i.e., what necessarily flows from the express teachings. I further understand that the mere fact that a certain thing may result from a given set of circumstances is not sufficient.

IV. STATE OF THE PRIOR ART

28. Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (EX-1001 1:22-24.) 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.) 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.) 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.)

29. 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.) 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.)

30. 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.) 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.)

31. Accordingly, there was a long-felt need for an improved forensic visibility technique to efficiently determine whether computer objects were malware.

V. THE '045 PATENT

A. Summary of the '045 Patent

32. 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.)

33. 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.)

34. 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.) 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.

35. 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.) 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.) 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, 47–53, 3:23–28 3:55–57, 8:9–19.).

36. 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.)

37. Thus, the '045 patent describes and claims systems and methods that provide more efficient and accurate identification of malware and improve the identification of other malware (and corresponding events) that might otherwise go

undetected in prior art systems, thereby improving system performance and reducing required resources. (EX-1001 1:15-19, 2:16 – 19, 23 – 38, 2:47-53, 3:23–28, 3:55-57, 8:9-19.)

B. Claim Construction

38. Petitioner concedes that no dispute exists 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"
1 ¹	"global perspective"	Not indefinite. Plain-and-ordinary meaning wherein the plain-and-ordinary meaning is "information about

¹ 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, I apply the Court's construction for "global perspective" in claim 1 for all claims that recite a "global perspective" limitation.

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

Claims	Claim Term	Court's Construction
		events related to the monitored even [sic] ² across a network”
1 ³	“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

² I understand “even” in the Court’s claim construction order as a typographical error that should instead recite: “event.”

³ 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, I apply 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, I 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.

C. Level Of Ordinary Skill In The Art

39. I understand that certain issues relating to the validity of the '045 patent must be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a “person having ordinary skill in the art” or “POSITA” that someone would have had at the time the invention as claimed was made. In deciding the level of ordinary skill, I have considered the following factors, which I have been informed are relevant in determining the level of ordinary skill in the art:

- The levels of education and experience of persons working in the field;
- The types of problems encountered in the art;
- The prior art solutions to these problems;
- The rapidity with which innovations are made; and

- The sophistication of the technology.

40. 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. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

41. I understand that Petitioner and its expert have defined the level of ordinary skill in the art as:

[A] person having ordinary skill in the art [] at the time of the earliest claimed priority date for the '045 patent would have had a bachelor's degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics such as malware/exploit detection and/or network forensics. More education can supplement practical experience and vice versa.

(Petition 8-9.)

42. Despite minor variations in these two positions, these variations would not alter my opinions expressed in this Declaration.

43. Based on either standard, I was at least a person of ordinary skill in the art at the time of the invention of the '045 patent.

VI. OVERVIEW OF PRIOR ART

A. Overview of Rockwood (EX-1004)

44. 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.”), ¶175 (“Rockwood discusses attacker profiles in terms of human actors. . . . A POSITA would have known that the human-centric attacker profiles, as disclosed by Rockwood, would be less useful for virus and/or worm attacks . . .”); *see also id.* ¶176.)

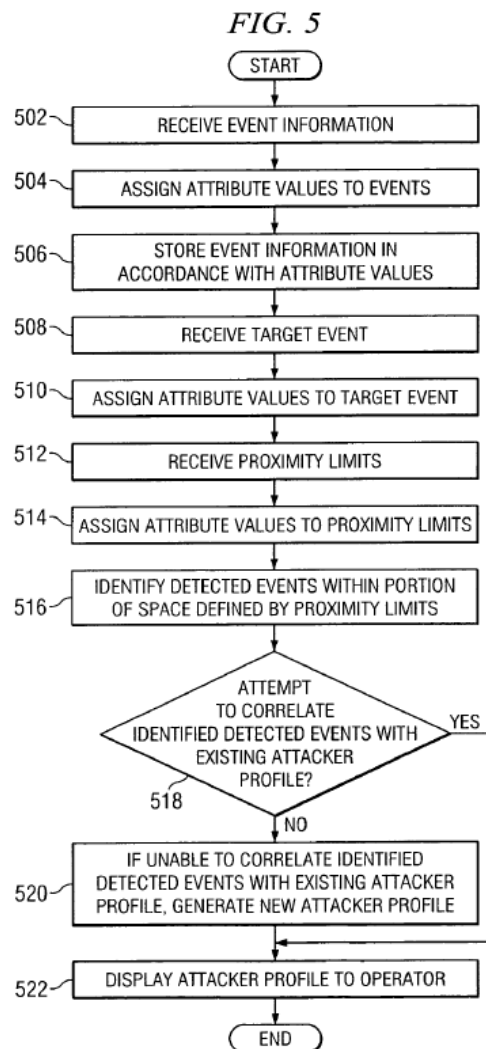
45. Rockwood performs data collection with a hardware configuration that uses sensors located at a network port that receives TCP/IP packets or other similar communications from network 100. (*See, e.g.,* EX-1004 2:40-45; 3:36–41; 14:52-57, Fig 1; Fig. 6.) Rockwood’s configuration matches the prior art system discussed

in the '045 patent, where sensors (i.e., 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 (“However, existing 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. . . . Accordingly, network edge devices ***have no ability to establish any sort of context from within the host or system that is generating the event.***”) (emphasis added).)

46. Rockwood's sensors are network edge devices that collect information transmitted through a network port. (EX-1004 3:36-49.) Unlike the '045 patent's collection agents, Rockwood's sensors do not collect information from within the endpoints, such as the contextual state information, regarding an observed event because they reside at the network edge. Thus, 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.

47. Rockwood processes events in isolation and does not trace the chain of events within an endpoint. Rockwood's event information processing is illustrated by Figure 5:



(EX-1004 Fig. 5.)

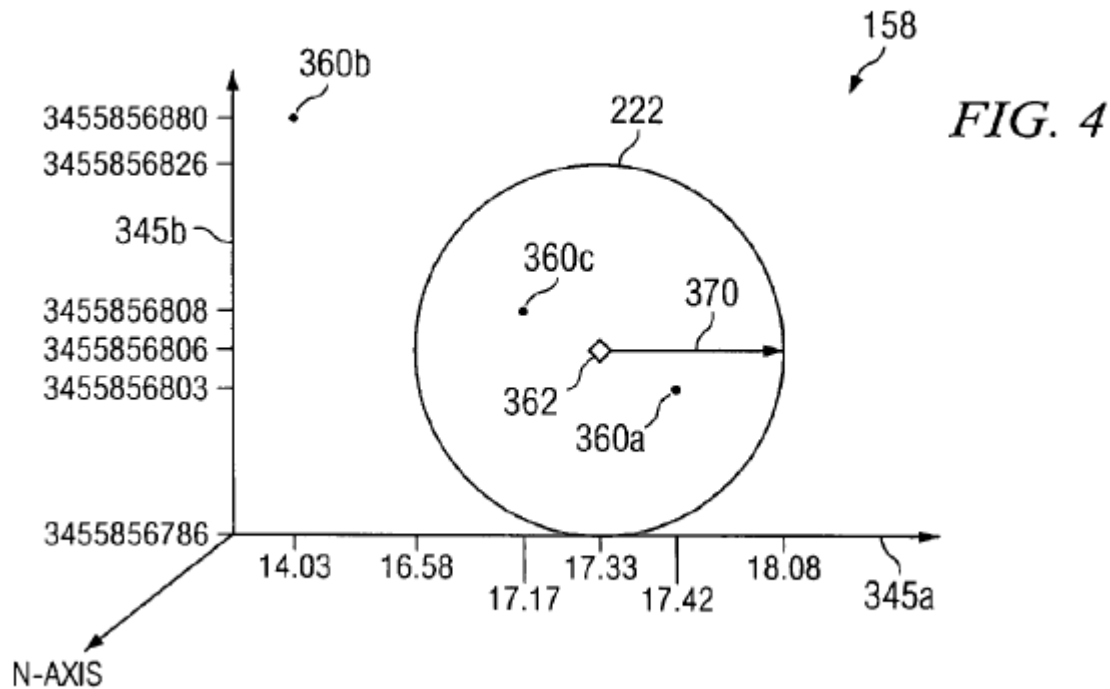
48. Rockwood abstracts each event into a point in n-dimensional space for subsequent analysis and forensic malware visualization. (EX-1004 Abstract, 1:40–56, Fig. 10.) The point is translated to an n-dimensional vector with n elements, where each element is an attribute of the event (e.g., time, IP address). (EX-1004 1:40-46, Figs. 3, 4.)

FIG. 3

	410a	410b	410c	420a	420b	420c
	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE VALUE	ATTRIBUTE VALUE	ATTRIBUTE VALUE
110a	DETECTED EVENT	5:25 P.M.	205.252.48.163	192.187.23.220	17.42	3455856803
110b	DETECTED EVENT	2:02 P.M.	205.252.48.240	192.187.23.206	14.03	3455856880
110c	DETECTED EVENT	5:10 P.M.	205.252.48.168	192.187.23.102	17.17	3455856808
364	TARGET EVENT	5:20 P.M.	205.252.48.166	192.187.23.110	17.33	3455856806
370	PROXIMITY LIMITS	45 MINUTES	20	30	0.75	20
						30

(EX-1004, Fig. 3.)

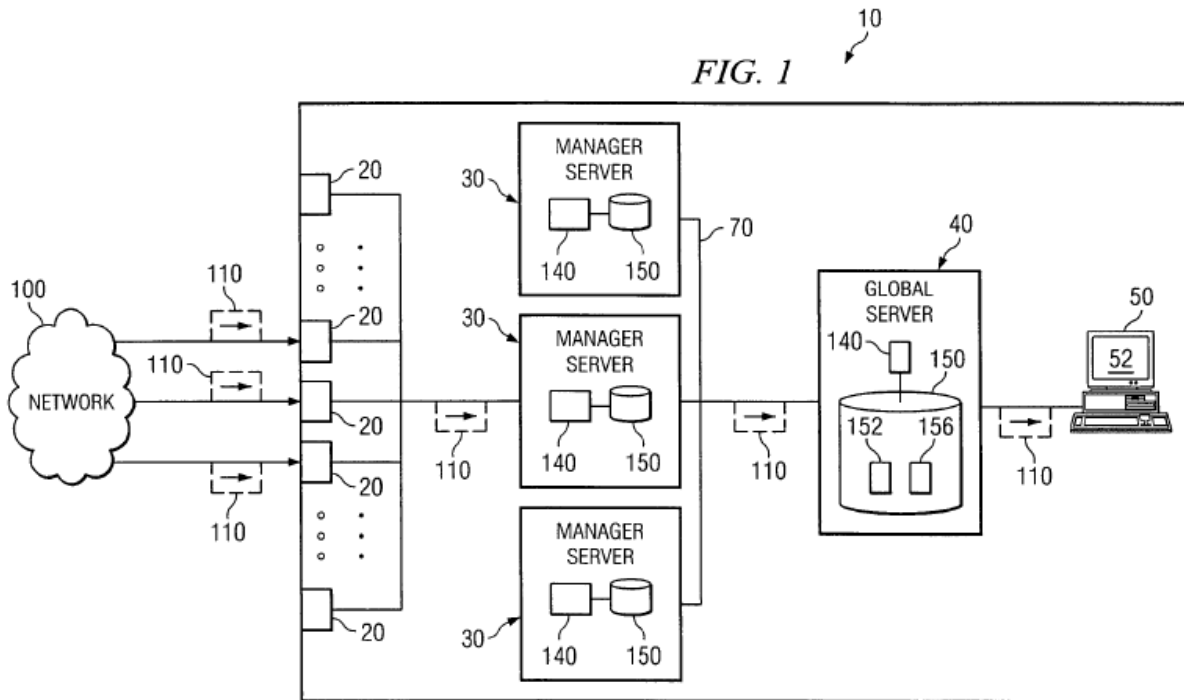
49. With these generated n-dimensional points, an incoming event can be compared against known malicious events based on the distance between the points that represent the incoming event and the malicious events. (See, e.g., EX-1004 1:46-46; 9:31-46, Fig. 4.)



(EX-1004 Fig. 4.)

50. Rockwood's "console" does not process event information. Rather, the console merely provides a user-friendly graphical user interface to display tailored and filtered information about detected events. (EX-1004 5:27-59 ("Intrusion detection system 10 may communicate the event information of detected events 110 to console 50 so that a user, such as an operator, may view and process the event information of detected events 110. . . . Console 50 may include a graphical user interface (GUI) 52 that tailor and filters the data presented to the user. Generally, GUI 52 provides the operator of console 50 with an efficient and user-friendly presentation of event information of detected events 110.")) Rockwood's event processing is

instead performed by backend servers (manager server 30 or global server 40), as illustrated by the intrusion detection system Fig. 1:



51. Rockwood's intrusion detection system "comprises a plurality of sensors 20, one or more manager servers 30, global server 40, and console 50." (EX-1004 2:40-48 ("Intrusion detection system 10 performs data collection using sensors 20. The data is correlated by manager servers 30 and/or global server 40.")). The manager server "represents any hardware or software module that controls or monitors one or more servant nodes, such as sensor 20. . . . [E]ach manager server 30 includes a correlation engine 140 and a ruleset 152 for receiving and correlating detected events 110 from sensors 20. Generally, through correlating and aggregating

detected events 110, manager server 30 is capable of detecting an attack or potential attack spread among sensors 20.” (EX-1004 4:5-17.) The global server “represents any hardware, software, firmware, or combination thereof operable to process, control, and monitor system 10 at the highest logical level” and, “[a]ccording to certain embodiments, global server 40 comprises a correlation engine 140. Correlation engine 140 is operable to correlate detected events 110 to detect an attack occurring upon or within the enterprise.” (EX-1004 4:39-67.)

B. Overview of Xie (EX-1005)

52. Xie is a Ph.D thesis titled “A Spatiotemporal Event Correlation Approach to Computer Security.” (EX-1005 1.) Xie addresses two separate applications of spatiotemporal event correlation: anomaly detection and network forensics. (EX-1005 1.) Anomaly detection is based on abnormal file changes *within a given computer*, and using those file changes to identify patterns of file updates that are shared across multiple hosts. (EX-1005 1.) In contrast, network forensics focuses on identifying the *source node* and *attack flows* (instead of source object) of detected malware based on statistical processing of network traffic. (EX-1005 1.)

1. Anomaly Detection Using Spatiotemporal Correlation

53. In Xie’s anomaly detection technique, the state change of a given computer (referred to in Xie as “state transition”) is abstracted into an n-dimensional

point or n-dimensional vector. (EX-1005 1, 25-26, 29-30.) Each element in this n-dimensional vector represents whether a selected file changes. (EX-1005 1, 25-26, 29.) In other words, the anomaly detection technique selects n files to monitor; and if any of them changes (for any reason, whether legitimate or due to malware), the element in the n-dimensional vector representing this file acquires a specified value (e.g., 0 or 1). (*See, e.g.*, EX-1005 25-26, 30, 33-34.)

54. Anomaly detection is then performed by monitoring the clustering of these n-dimensional points. For legitimate file changes, the n-dimensional points tend to cluster around a known location. (EX-1005 30.) In contrast, file changes caused by malware tend to create abnormal clusters. (*See, e.g.*, Figure 2.1 at EX-1005 31.). This is illustrated in Xie by Figure 2.1, below:

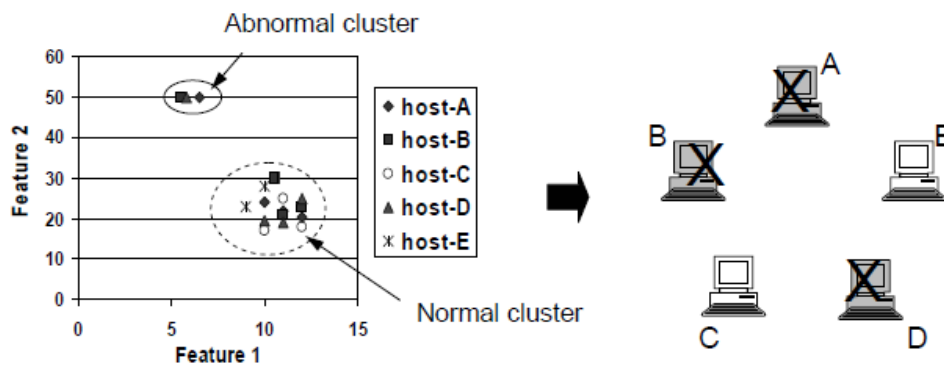


Figure 2.1: Pointillist approach to anomaly detection. Normal points are clustered by the dashed circle. The appearance of a new cluster consisting of three points suggests anomalous events on host A, B, and D.

55. 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.

2. Network forensics using spatiotemporal event correlation

56. Xie's network forensics technique aims to identify the true source, i.e., the original computer, of an internet attack, especially when "indirection" (e.g., using "stepping stones" or "zombies") is involved. (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," 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.)

57. 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 67, 128.)

58. Xie's network forensics technique generates a ***causal tree*** between ***different computers*** in a network. (See, e.g., EX-1005 63, 62-63, Figs 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.

59. 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 78, Figure 3.12 (where the traffic is collected from the ***backbone*** of a university network).) 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.

VII. ROCKWOOD IN VIEW OF XIE DOES NOT DISCLOSE OR RENDER OBVIOUS THE CHALLENGED CLAIMS

60. 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
-----------------	-------------	---	-------------

61. As discussed above, I apply the plain and ordinary meaning of all claim terms, including the district court's clarifying comments, consistent with the district court's claim construction order.

62. I disagree with the arguments in the Petition and the opinions set forth by Dr. Nielson for at least the reasons that I discuss in further detail below: Petitioner's arguments based on the combination of Rockwood in view of Xie are unlikely to succeed because:

- (1) Petitioner relies solely on Rockwood regarding 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]. Petitioner presents two alternative arguments. First, Petitioner argues that the operating system or network layer discussed in Rockwood corresponds to the claimed "first object acting on a target." However, an operating system or network layer is not consistent with the plain and ordinary meaning of an "object" in the computer context or the requirements for the "object" claimed in the '045 patent. Second, Petitioner argues in the alternative that the data/code package discussed in Rockwood corresponds to the "first object acting on a target." However, Rockwood's data/code package is a packet intercepted during transmission, and thus does not indicate whether it ever subsequently arrived at its target, much less whether it ever 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 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 disclose or teach collecting the 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]. There is no disclosure or teaching in either Rockwood or Xie of 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.

A. Rockwood's Does Not Gather Information about Objects Acting on Targets or Executing on Devices

63. Claim limitations 1[b], 10[g], and 17[g] each require gathering an event defining an action of a first object. (EX-1001, cls. 1, 10, 17.) Claim 1[b] includes the additional limitation “*wherein the first object is executed on a device.*” Petitioner relies only on Rockwood for these limitations. (See Petition 14-17.) Petitioner's grounds do not disclose or render obvious these limitations because Rockwood does not gather event information about an object acting on a target or executing on a device.

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>

1. The “Network Layer/OS” Is Not a “First Object”

64. Petitioner incorrectly asserts that 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 (“A PHOSITA would have understood that the network layer / OS (‘first object’) executes on a device . . .”).) 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.

65. The context of the claim language in the '045 patent shows that the network layer/operating system cannot be the “first object.” 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 the “originating object of the first object” in order to generate contextual state information. (See EX-1001 Claim 1[c]; *see also* Section VII.B, *supra*.)

66. Petitioner does not identify any disclosure in Rockwood (or anywhere else in the prior art) of an originating object of an operating system or network layer. Instead, Petitioner argues that the originating object is Rockwood's “attacker profile.” (Petition 17 (“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’”); *see also id.* at 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 nonsensical. (*See* Petition 17-18.) 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."

67. Claims 1 and 8 further illustrates why neither the network layer nor the operating system satisfy the "first object" limitation. 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."

68. 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.) 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.

69. Thus, Petitioner’s first argument that the “first object” is the network layer and/or operating system is thus wrong and should be rejected for all limitations for which petitioner relies on this mapping. (*See* Petition 14, 17, 21-22, 29, 38, 39, 46, 55-56, 60, 66 (relying on a network layer/OS mapping of “first object”).)

**2. Rockwood Does Not Disclose or Render Obvious an Event
Defining a First Object Acting on a Target**

70. 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 likewise fails to identify any disclosure

or teaching of an “event defining an action of a first object acting on a target.” Rather, Petitioner wrongly argues that transmitting executable malware is the same as the claimed gathering an event defining an action of a first object acting on a target. (Petition 16 (citing EX-1004 3:50-60, 12:35-45 and EX-1002 ¶¶153-160).)

71. Transmitting information to a particular destination does not define “an action of a first object acting” on that destination. The '045 Patent describes the claimed “action” on a target as an event type, such as a registry edit, that has been determined to have been performed on a target. (EX-1001 17:20-29.) By contrast, Rockwood describes collecting event information from processing 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.”).) 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 thus cannot indicate whether its contents (i.e., the data/code package petitioner maps as the first object) ever takes any action on an intended target.

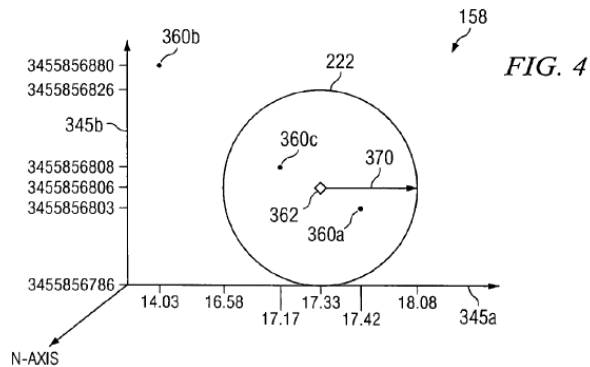
72. None of the Rockwood excerpts Petitioner cites describe an object acting on a target. Petitioner's first citation describes the operation of network edge sensors, which "may use algorithms, signatures, scripts, or any suitable detection or comparison technique to process packet headers, packet payloads, and/or any other data." (Petition 16 (citing EX-1004 3:50-60).) This information about the operation of Rockwood's sensors does not disclose or render obvious gathering 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.

73. Likewise, Petitioner's second citation 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. Operator 60 of system 10 wants to determine whether any detected events 110 in detected event storage 158 may be related to this attack."))).) This enemy attack event is depicted in Figures 3 and 4.

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

FIG. 3

	410a	410b	410c	420a	420b	420c
	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE	ATTRIBUTE VALUE	ATTRIBUTE VALUE	ATTRIBUTE VALUE
110a	DETECTED EVENT	5:25 P.M.	205.252.48.163	192.187.23.220	17.42	3455856803
110b	DETECTED EVENT	2:02 P.M.	205.252.48.240	192.187.23.206	14.03	3455856880
110c	DETECTED EVENT	5:10 P.M.	205.252.48.168	192.187.23.102	17.17	3455856808
364	TARGET EVENT	5:20 P.M.	205.252.48.166	192.187.23.110	17.33	3455856806
370	PROXIMITY LIMITS	45 MINUTES	20	30	0.75	20
					30	



Rather, it describes an attack event using information about the source IP address, the destination IP address, and timestamp, as well as attribute values 420a, 420b, and 420c that represent the normalized values for attributes 410a, 410b, 410c, respectively. (See EX-1004 16:62–17:16.) None of these values indicate a computer object’s action on a target. The intercepted data/code package is only transmitted to another computer, but Rockwood does not disclose “an action” of the data/code package (the “first object” under Petitioner’s second theory)—for example, an action on the target device and its IP address (the alleged “target,” according to Petitioner (Petition 27)). (See EX-1004 Fig. 3 (illustrating “a table of event information,” which does not include a computer object’s action or an identification of any

computer object acting on a target).) Simply put, even if POSITA could understand this event as an attack based on the transmission of a computer object, there is no disclosure or teaching of gathering information about this event that includes actions taken by a first object on a target.

74. Moreover, Rockwood's defines "attack" without regard to whether any computer object acts on any 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.")) In other words, Rockwood's "attack" events include attempted, but failed, transmissions of computer objects that never reach or act on a target within the protected network. Accordingly, Petitioner's suggestion that Rockwood's detection of an attack event implies that a computer object must have acted on a target is incorrect.

75. 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.” Petitioner’s first argument fails because a network layer/operating system cannot be the claimed first object. Petitioner’s second argument fails because Rockwood/Xie do not disclose the alleged first object (a “data/code package”) as acting on any target.

B. The Rockwood-Xie Combination Does Not Disclose or Render Obvious the “Originating Object”

76. 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.) Petitioner’s Rockwood-Xie combination does not disclose or render obvious this limitation.

Claim Limitation	Claim Language
1[c]	<i>“generating contextual state information for the event by correlating the event to an originating object of 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 <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>

77. The claims recite a “contextual state” that includes “an indication of the originating object of the first object.” (EX-1001 cls. 1[c], 8[h], 16[h].) In addition, the contextual state is generated by “correlating” events “to an originating object.” 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.”).) Petitioner fails to identify any disclosure or suggestion of the claimed “originating object” in the Rockwood-Xie combination.

1. Rockwood Does Not Disclose or Render Obvious the Claimed “Contextual State” and “Originating Object”

78. As discussed above, the claims recite an “originating object” that originates a first object. Petitioner’s “first mapping” assumes that the network layer/OS in Rockwood is the “first object” but that mapping fails because Petitioner identifies no object that originates the network layer/operating system. Indeed, Petitioner incorrectly identifies the “originating malware” as the originating object. (Petition 17-18 (“Xie teaches identifying originating malware of an attack “originating object”) (e.g., that causes a network layer/OS (“first object”) to transmit malware”).) The originating malware does not originate the network layer/operating system.

79. Petitioner's "second mapping" similarly fails to identify the claimed originating object. In this mapping, the "first object" and the "originating" object" are the same thing. Petitioner identifies the malware as the originating object ("originating malware") and the same malware being transmitted ("transmitted malware") as the first object. (Petition 19.) Petitioner does not show how the malware initiates or creates a first object.

80. In addition, Petitioner wholly fails identify or explain how Rockwood discloses or renders obvious generating a contextual state "by correlating the at least one event to an originating object." Petitioner asserts that Rockwood's "attacker profile" is used "to correlate an event to an originating object/process of the first object." (Petition 17.) But the attacker profile does not even identify, much less "correlate" an event to, an originating object/process. Rockwood's attacker profile is simply a data structure with a collection of information that "comprises a plurality of characteristics of an attacker of an enterprise's computer network. In certain embodiments, existing attacker profile 224a includes name and background information such as, for example, last known residence or last known employer." (EX-1004 10:8-22.) In short, the attacker profile simply provides information about a person or entity that is attacking the network (*See* EX-1004 8:20-22 ("By determining the identity of an attacker, operator 60 may be able to preempt future attacks.")).) It does not correlate

an event to an originating object of the attack. Neither the attacker profile nor the identity of an attacker is an originating object of the attack.

**2. Xie Does Not Teach the Claimed “Contextual State” and
“Originating Object”**

81. Petitioner cannot make up for Rockwood’s shortcomings by relying on Xie. First, Petitioner incorrectly contends that “Xie teaches identifying originating malware of an attack (‘originating object’) (e.g. that causes a network layer/OS (‘first object’) to transmit malware)” (Petition 18.) Xie does not disclose the claimed “originating object” for the same reasons stated above for Rockwood.

82. Second, Xie does not disclose generating a contextual state by “correlating the at least one event to an originating object.” Petitioner wrongly asserts 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.) Xie does not “identify” the name and location of originating malware at all, much less by using “correlations” of network events. 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. The Lion worm was found in early 2001 We configured the isolated cluster with three Lion vulnerable hosts and one additional machine that launched the worm.”.) In other words, the name and type of malware, the Lion Worm, was known from the beginning and did not need to be determined by correlating anything. The Seurat system did not independently identify the Lion worm amongst other possible computer objects that could have been responsible for illustrative malware attacks.

83. Third, Xie does not disclose or teach a contextual state that includes “an indication of the originating computer object of the first object.” Petitioner does not identify any disclosure from Xie (or Rockwood) discussing identifying, analyzing, or attempting to determine how computer objects may be related to other computer objects. (*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 a potentially suspicious file 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.

84. Rather, Xie discloses identifying infected “host devices” using information about file system changes, such as to their file size. (EX-1005 47-49.) A “host device” is not an originating object—let alone the originating object of the network layer/OS (first object for the first mapping). (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.”).) Nor is it transmitted malware (first object for the second mapping). (*See* Section VII.A., *supra*.) Thus, Petitioners’ reliance on the Xie host device does not render any claim obvious.

85. Petitioner’s proposed combination for this limitation, i.e., “includ[ing] the file change correlations of Xie with the correlations of Rockwood and include Xie’s originating malware information in Rockwood’s attacker profile” (Petition 20) does not disclose or render obvious the claimed “contextual state” or “originating object.” 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.

C. Rockwood Does Not Obtain a Global Perspective for the Event

86. 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.) Petitioner does not contend that Xie discloses this limitation and relies on Rockwood alone.

Claim Limitation	Claim Language
1[d]	<i>“obtaining 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>
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>

87. Petitioner incorrectly asserts that Rockwood’s “global view” is the “global perspective” recited by the claims. (Petition 21-22, *see also* 23-25.) The claims require the “global perspective” to be specific to an event. An event-based global perspective is an explicit claim requirement. (*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”); 1[d], 8[i] (“wherein the global perspective for one or more related events to the at least one event across a network.”).) 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.)

88. Petitioner fails to establish that Rockwood in view of Xie meets the requirements of the claim language reciting obtaining a global perspective for an event...which includes information about related events across a network.

89. Rockwood fails to disclose or suggest obtaining the recited event-specific “global perspective.” 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 Xi) (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.) The only “global view” Rockwell discloses is for the *state of a computer system*, not a particular monitored *event* as claimed. (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”); 19:27-31 (“According 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”).) 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.) Petitioner does not even contend that Xie discloses a global perspective across a network. Petitioner fails to

explain how a PHOSITA would transform a general view of the overall state of a computer system into the particular claimed global perspective for an event obtained from particular information and includes information about related events across a network, whether modified by Xie or otherwise.

90. Petitioner fares no better with its conclusory argument that “a PHOSITA 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 vague contention fails to explain how Rockwood’s network-level aggregation of system information discloses or renders obvious the claimed obtaining of a “global perspective” of a particular monitored *event* in relation to other events across a network or how Xie’s localized lion worm testing somehow transforms Rockwood’s network aggregation into the claimed “global perspective.” A general network-level aggregation of system information does not equate with obtaining the claimed global perspective, which involves a global perspective for a particular event obtained through specific information about a first object and an originating object and 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*.”).) Petitioner offers no explanation how the aggregated information in

Rockwood represents a particular monitored event or how such an event may be determined to be related to other events across a network for purposes of obtaining the claimed global perspective. (See Petition 21-26.) This vague and conclusory argument should be rejected.

91. First, Rockwood uses the term “global view” *once*, but does not disclose how the global view is generated, what it includes, and what it relates to. (EX-1004 14:29.) As a result, there is no disclosure or teaching that the global view is obtained based on the contextual state, no disclosure that the global view includes information associated with the first object or originating object, and no disclosure that the global view relates to *events* related to the event across a network. Petitioner’s reliance on Rockwood’s “global view” is vague and misplaced, because it fails to address why or explain how a POSITA would understand Rockwood’s network-level aggregation of information to disclose or render obvious the claimed “global perspective.”

92. As a result, it is my opinion that Rockwood does not teach that its “global view” discloses or teaches a global perspective for a monitored event that includes information about one or more related events across a network.

D. Rockwood / Xie does Not Disclose or Render Obvious the Claimed Event Line

93. 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 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>

94. 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.

95. 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]; *see* Petition 26 (citing EX-1004 5:48-51, 7:3-10, 7:20-22, 10:34-44, 16:62-66).) Rockwood's attacker profile, even as modified by Xie as Petitioner claims, does not include an indication of the claimed originating object. (*See* Section VII.B., *supra*.)

96. Petitioner does not identify any disclosure showing, or explaining how, any of the information displayed on Rockwood's GUI display of an attacker profile—which relates to an individual who is responsible for an attack—could be modified to display an event line with the fields of information required by the claims. (*See* EX-1004 10:4-22 ("Each existing attacker profile 224a comprises a plurality of characteristics of an attacker of an enterprise's computer network.... For example, a particular existing attacker profile 224a may correspond to an individual who typically launches attacks between 5:00 p.m. and 5:30 p.m. using external computers with IP addresses between 205.252.48.160 and 205.252.48.200.")) Xie does not

disclose or render obvious a GUI that displays the fields of information required by the claims—and notably, no indication of an “originating object.”

97. Beyond those obvious deficiencies, Petitioner clearly fails to identify sufficient disclosure in either Rockwood or Xie of event details that include “uniquely identifying the first object, the action of the first object, the target, the originating object, and global perspective information. Petitioner clearly identifies the “attacker profile” as the “originating object” for this claim limitation – “For example, Rockwood discloses displaying the attacker profile (“originating object”) on the GUI in connection...” (Petition 26.) But the “attacker profile” is not the “originating object” that Petitioner identified in prior limitations for either mapping. For example, for the generating a contextual state limitation (1[c]), Petitioner identifies the “originating malware” as the “originating object” in both mappings. (Petition 17 (“In the first mapping... A PHOSITA would have recognized that the sources of attack or originating malware (corresponding to ‘originating object of the first object’”)); Petition 19 (“In the second mapping ...[t]he above-discussed source of attack/originating object is the originating malware (‘originating object’)).)

98. In addition, the attacker profile is not an originating object and Petitioner does not even attempt to show how the attacker profile creates or initiates

other objects. Rather, as discussed above, Rockwood's attacker profile is simply a data structure with a collection of information that "comprises a plurality of characteristics of an attacker of an enterprise's computer network. In certain embodiments, existing attacker profile 224a includes name and background information such as, for example, last known residence or last known employer." (EX-1004 10:8-22.) In short, the attacker profile simply provides information about a person or entity that is attacking the network (*See* EX-1004 8:20-22 ("By determining the identity of an attacker, operator 60 may be able to preempt future attacks").) Neither the attacker profile nor the identity of an attacker is an originating object of the attack

99. Based on the foregoing, it is my opinion that Petitioner fails show that Rockwood in view of Xie discloses or renders obvious limitations 1[e], 8[j], and 16[i].

E. A POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art

100. A POSITA would not have been motivated to combine Rockwood and Xie because each reference suffers from an inability to collect contextual information regarding an observed event from within the host or system that is generating the event. (*See* Section IV, *supra*.) 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.)

101. Neither Rockwood nor Xie collect information about an event from host computers, and instead rely on intercepting network transmissions outside the host computers using sensors along the network's communications pathways. (See Section VI.A-B, *supra*.)

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*.) 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 19-20.) 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 originated other computer objects.

103. Given the stark differences between these references and the claimed invention—particularly in view of the '045 patent's instruction that network edge devices are insufficient—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.

F. Dependent Claims

104. 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.

VIII. CLAIMS AND/OR LIMITATIONS NOT ADDRESSED IN THIS DECLARATION

105. It is my understanding that this declaration is being provided in support of Patent Owner's Preliminary Response. I have provided analysis of key limitations not included in the prior art. The fact that I have not analyzed particular limitations or claims in no way indicates or supports that these limitations or claims are disclosed or rendered obvious by the prior art, and I reserve the right to supplement my analysis if asked to do so.

IX. SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS

106. I understand that in determining obviousness of a claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, commercial success, etc. I further understand that these indicia constitute independent evidence of nonobviousness that can be the most probative in that regarding "in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements."

107. As discussed by my summary of the prior art above, there was at least a long-felt and persistent need existed to improve network forensics methods before the invention of the '045 patent. (*See* Section IV, *supra*.) Prior attempts to develop

reliable network security were limited in their ability to establish any sort of context or obtain useful information from within the host or system, making them insufficient to identify and address the threats faced by modern computer networks. (*See* Section IV, *supra*.) Where others failed, the inventors of the '045 patent succeeded. (*See* Section IV, *supra*.)

108. Patent Owner currently accuses at least four industry participants, including Petitioner, of infringing the technology claimed in the '045 patent, demonstrating the critical need and widespread industry reliance on these novel methods. (*See* EX-2017; EX-2015; EX-2016; EX-2018.) Petitioner, in particular, markets and provides Trend Micro's XDR technology, the components of which practice the system and methods claimed in the '045 patent. (*See* EX-2017.)

109. These secondary indicia further support my opinion that the '045 patent was nonobvious.

X. CONCLUSION

110. For at least the foregoing reasons, it is my opinion that Petitioner's ground does not render obvious any of the challenged claims of the '045 patent.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information

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

and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

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

Executed this 10th day of August, 2023 in Los Angeles

Respectfully submitted,



Nenad Medvidovic, Ph.D.