

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,
Petitioner

v.

WEBROOT INC.,
Patent Owner.

IPR2023-00657
Patent 10,257,224 B1

Before PATRICK M. BOUCHER, MICHELLE N. WORMMEESTER, and
AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	Background.....	1
B.	Related Matters.....	1
C.	The '224 Patent.....	2
D.	Illustrative Claims.....	4
E.	Asserted Ground	7
II.	ANALYSIS.....	7
A.	Level of Ordinary Skill in the Art	7
B.	Claim Construction	8
C.	Obviousness	9
1.	Summary of Rockwood.....	9
2.	Summary of Xie.....	12
3.	Analysis.....	13
a.	Petitioner's "First Mapping".....	13
b.	Petitioner's "Second Mapping"	17
III.	CONCLUSION	20
IV.	ORDER.....	20

I. INTRODUCTION

A. *Background*

Trend Micro Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting institution of an *inter partes* review of claims 1–20 of U.S. Patent No. 10,257,224 B1 (Ex. 1001, “the ’224 patent”). Open Text Inc. (“Patent Owner”) filed a Preliminary Response (Paper 6, “Prelim. Resp.”).

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

Upon consideration of the Petition in view of the present record, and for the reasons explained below, we determine that Petitioner has not shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims. We accordingly do not institute an *inter partes* review of claims 1–20 of the ’224 patent.

B. *Related Matters*

The parties identify the following district court cases as related to this proceeding:

Webroot, Inc. et al. v. Trend Micro Inc.,
Case No. 6:22-cv-00239 (WDTX);

Webroot, Inc. et al. v. Sophos Ltd.,
Case No. 6:22-cv-00240 (WDTX);

Webroot, Inc. et al. v. CrowdStrike, Inc. et al.,
Case No. 6:22-cv-00241 (WDTX); and

Webroot, Inc. et al. v. AO Kaspersky Lab,
Case No. 6:22-cv-00243 (WDTX).

See Pet. 2; Paper 4, 1.

We instituted an *inter partes* review of claims 1–4, 7–8, 10–13, and 16–19 of the ’224 patent in IPR2023-00126.

C. *The '224 Patent*

The '224 patent describes “methods and systems for providing forensic visibility into client systems.” Ex. 1001, 1:18–19. The patent explains that “existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic,” such as hostnames, ports, protocols, and IP addresses. *Id.* at 1:36–38. Such tools, however, “tend to receive network events outside of a host or system” and “have no ability to establish any sort of context from within the host or system that is generating the event.” *Id.* at 1:41–42, 46–48. Thus, the edge devices have no way of knowing to what extent a virus may have impacted a device, what files may have become infected, and/or what processes and/or objects operating are linked to the virus. *See id.* at 2:14–18.

The patent describes methods “whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event.” Ex. 1001, 2:26–29. As an example, “a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network.” *Id.* at 2:29–32.

Figure 6 provides a flowchart of a method for providing forensic visibility that corresponds to the challenged independent claims:

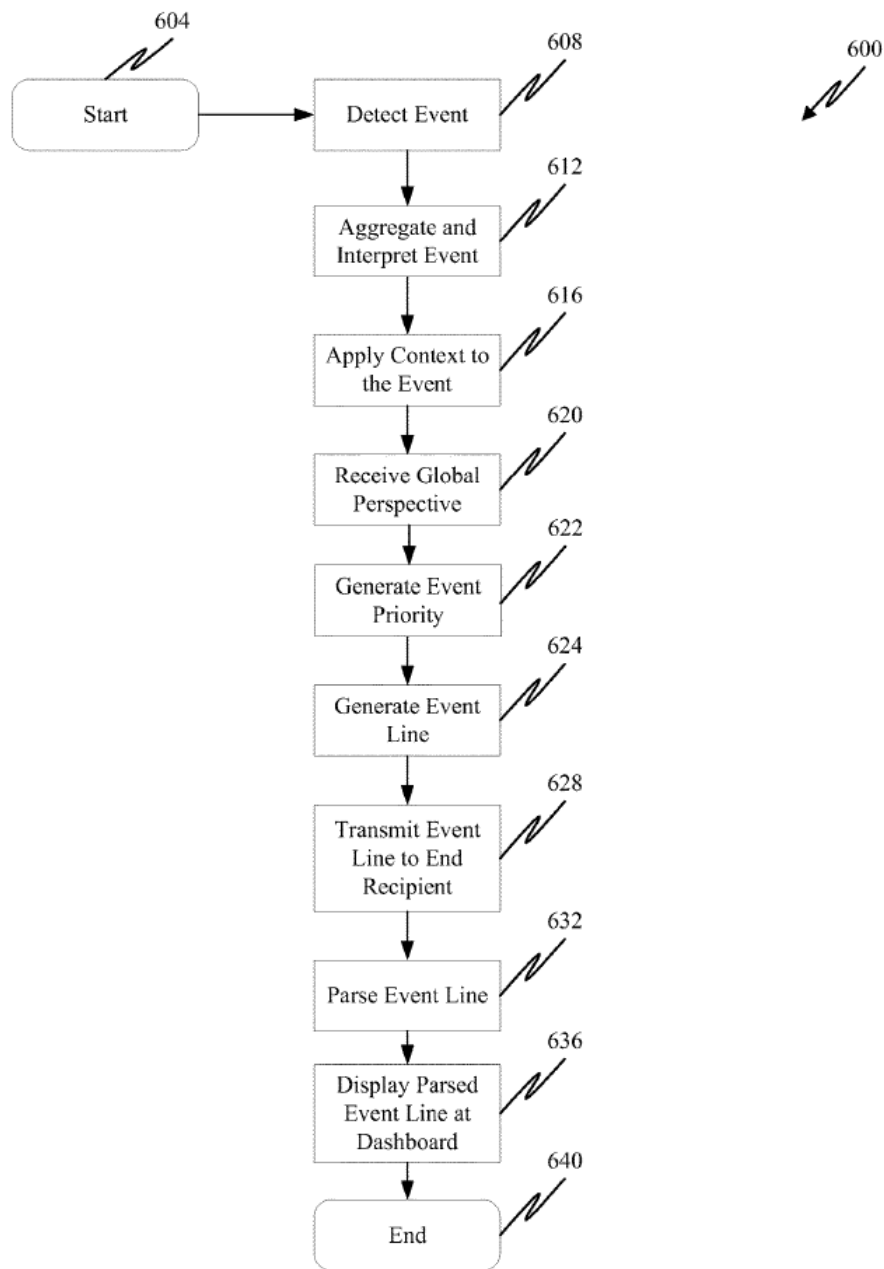


Figure 6 is a Flowchart of One Embodiment of the Patented Method

The method is initiated at step 604, and an event may be detected at step 608 “by one or more system filters 340 of a sensor agent 208.” Ex. 1001, 18:28–29. At step 612, “local aggregator and interpreter 344 receives

events from the low level system filters 340,” and, at step 616, “a contextual state may be applied by a context analyzer 348 to the event information.”

Ex. 1001, 18:49–52, 59–60.

Once the contextual state is applied, “a global perspective is applied for each event and/or each object of the event and contextual state” at step 620. Ex. 1001, 18:67–19:1. The “global perspective” may include “information related to the age, popularity, and determination of an object—whether it is known good, bad, or unknown” and “information pertaining specifically to an IP/URL address,” including “network activity and an assessment of the reputation and category of each website and IP address.” *Id.* at 19:2–9.

At step 622, “an event priority may be applied to the event.” Ex. 1001, 19:11–12. “[T]he event priority may be obtained . . . applying [a] rule set to aggregated event information, contextual state information, and global perspective information” and, at step 624, “such data is appended to each relevant portion of an event line.” *Id.* at 19:12–17. At step 628, the event distributor may “transmit the event line . . . to the end recipient.” *Id.* at 19:18–20.

D. Illustrative Claims

Challenged claims 1, 10, and 17 are independent. Claim 1 is directed to a method and claim 10 is directed to a system that corresponds closely to the claim 1 method. Claim 17 is also directed to a system, but differs somewhat in that it merges and modifies the “contextual state” and “global perspective” limitations.

The independent claims are reproduced below:

1. A method comprising:

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 wherein the global perspective relates to one or more other events related to the event across a network;

generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated event line.

10. A system for providing forensic visibility into a system, comprising:

a device comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

generate contextual state information for the event by correlating the event to an originating object of the first object;

obtain 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 wherein the global perspective relates to one or more other events related to the event across a network;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

17. A system for providing forensic visibility into a system, comprising:

a first device comprising:

a communication interface;

a processor;

data storage; and

a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

gather an event defining an action of a first object acting on a target;

determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object;

generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmit the generated event line utilizing the communication interface.

Notably, although the independent claims generally correspond to the method shown in the Figure 6 flowchart, they omit step 622, which applies a priority to the event by applying a rule set to the aggregated event information, contextual state information, and global perspective information. In the independent claims, nothing is done with the “global perspective.”

E. Asserted Ground

Petitioner asserts that the challenged claims are unpatentable on the following ground:

Claims Challenged	35 U.S.C. §	References/Basis
1–20	103(a)	Rockwood ¹ and Xie ²

See Pet. 5.

Petitioner also relies on a Declaration of Seth James Nielson, filed as Exhibit 1002. Patent Owner relies on a Declaration of Nenad Medvidovic, Ph.D., filed as Exhibit 2001.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that one of ordinary skill in the art “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” and that “[m]ore

¹ U.S. Patent No. 7,352,280 B1 (Ex. 1004).

² Xie, *Thesis: A Spatiotemporal Event Correlation Approach to Computer Security*, Carnegie Mellon University (August 2005) (Ex. 1005).

education can supplement practical experience and vice versa” Pet. 10 (citing Ex. 1002 ¶ 97).

Patent Owner asserts that one of ordinary skill in the art “had a bachelor’s degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline” and “2–3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security.” Prelim. Resp. 26 (citing Ex. 2001 ¶ 40). Petitioner further asserts that “[m]ore advanced degrees and/or training in a related discipline can compensate for shorter work experience.” *Id.*

As Patent Owner does not dispute Petitioner’s characterization of the level of skill in the art, and because we find it generally consistent with the disclosures of the ’224 patent and the prior art, we adopt it for purposes of this analysis.

B. Claim Construction

Petitioner states that “all claim terms should be given their plain and ordinary meanings.” Pet. 10. Patent Owner asserts that all terms should be given their plain and ordinary meaning, and that claim 1 should be construed “to require generating contextual information before obtaining the global perspective.” Prelim. Resp. at 24–26.

We find that we need not construe any terms to reach a decision on institution in this proceeding. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

C. Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

Obviousness is resolved on the basis of underlying facts, including (1) the level of skill in the art, (2) the scope and content of the prior art, (3) the differences between the claimed subject matter and the prior art, and (4) any secondary considerations, including commercial success, long-felt but unsolved need, failure of others, and unexpected results. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

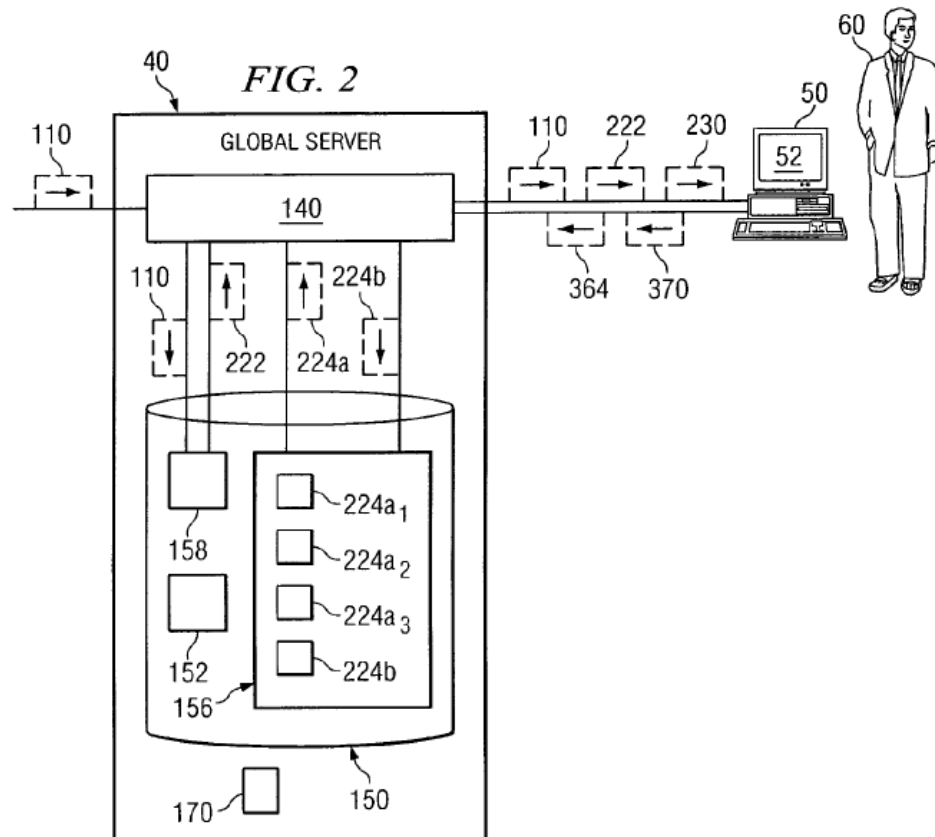
1. Summary of Rockwood

Rockwood is a U.S. patent directed to intrusion detection systems that may be “used by an enterprise to detect and identify unauthorized or unwanted use (commonly called an attack) of the enterprise’s computer network, which normally comprises a large number of nodes and network operations centers.” Ex. 1004, 1:15–19.

One disclosed embodiment is a method for correlating event information that involves receiving event information with attributes for “detected events,” assigning “attribute values” to each detected event, where the attribute values define a point in n-dimensional space, and storing the detected event information in accordance with the attribute values. *See* Ex. 1004, 1:36–46. The method then receives a “target event” with attributes comprising a plurality of attributes and attribute values defining a target point in n-dimensional space, receiving a plurality of “proximity limits” that

define a portion of n-dimensional space surrounding the target point, and identifying detected events with attribute values that are within the defined portion of the n-dimensional space. *Id.* at 1:46–56.

FIG. 2, reproduced below, is used to illustrate the operation of one embodiment:



“FIG. 2 illustrates a flow of operation among various components of [an intrusion detection system].” Ex. 1004, 2:13–14.

“Global server 40 receives detected events 110, such as from manager servers 30,” where “[e]ach detected event 110 comprises a plurality of characteristics such as, for example, time, source IP address, and destination IP address,” which “are referred to as attributes 410.” Ex. 1004, 5:61–66.

“Correlation engine 140 processes each detected event 110 according to attributes 410 of that detected event 110 . . . assign[ing] attribute values

420 . . . to each detected event 110 according to the particular attributes 410 of that detected event 110.” Ex. 1004, 5:61–66. Then, “[c]orrelation engine 140 uses rules stored in ruleset 152 to determine which attribute values 420 to assign to a particular detected event 110.”

Rockwood also describes how the system “is operable to determine the likely identity of an attacker by correlating identified detected events 222 with one or more existing attacker profiles 224 a stored in profile set 156.” Ex. 1004, 10:1–4. An “attacker profile 224 a comprises a plurality of characteristics of an attacker of an enterprise’s computer network” and may include “name and background information such as, for example, last known residence or last known employer.” *Id.* at 10:9–13.

Rockwood describes an example³ in which a global server receives a detected event, which occurred at 5:25 p.m. and originated from a UNIX-based computer. The correlation engine assigns the detected event appropriate attribute values and stores the detected event.

In the example, an attacker attempts to hack into a system to obtain sensitive information, the system identifies the attack as a detected event that occurred at 5:20 p.m. and originated from a UNIX-based computer. The detected event contained a segment of code signifying that it was an attack. The operator wants to determine whether any other detected events in storage might be related to this attack—in particular, whether any other detected events occurred within forty-five minutes of 5:20 p.m. and originated from UNIX-based computers. The operator thus selects the detected event as a target event, the console sends the target event to the

³ See Ex. 1004, 12:18–13:24.

global server, and the operator enters “forty-five minutes” and “Unix-based computer” into the console as proximity limits.

The correlation engine then identifies detected events in storage that correspond to points within the proximity limits of the target point and attempts to correlate the detected event with attacker profiles. The profiles include one for an attacker known to typically attack between 5:00 p.m. and 5:30 p.m. from UNIX-based computers and, because the attacker profile matches the attributes of the target event, the correlation engine correlates the target event with the attacker profile. The global server then sends the attacker profile to the console, which displays it to the operator, allowing the operator to learn the identity of the individual or organization that likely caused the target event.

2. *Summary of Xie*

Xie is a thesis that “explores a new spatiotemporal event correlation approach to capture the abnormal patterns of a wide class of attacks, whose activities, when observed individually, may not seem suspicious or distinguishable from normal activity changes.” Ex. 1005, 3. In pertinent part, the paper addresses “anomaly detection,” with a “‘pointillist’ method to detect similar, coincident changes to the patterns of file updates that are shared across multiple hosts” that is “performed by clustering points, each representing an individual host state transition, in a multi-dimensional feature space.” *Id.*

The thesis explains that because “[m]any attacks install new files on a compromised host, or modify files that are infrequently updated, . . . [v]arious information such as host file updates, file update times, and file size changes can be used as indicators” of attacks. Ex. 1005, 33. The

system generates vectors corresponding to host file updates over a one-day detection window and then correlates those vectors with vectors generated for each host over preceding days based on the distances between the vectors. *See id.* at 34.

Xie's method then clusters the vectors based on the distance between every pair of them, calling a cluster "new" if it consists of multiple vectors only from the detection window. *See Ex. 1005, 38.* "The appearance of a new cluster indicates [that] a change in file update patterns occurred during the detection window and should raise an alarm." *Id.*

Once the system detects a new cluster, it can identify the involved hosts and the files from which the cluster resulted. *See Ex. 1005, 39.* Then, "[b]ased on the suspicious hosts and the selected files for explaining root causes, system administrators can decide whether the updates are known administrative updates that should be suppressed, or some abnormal events that should be further investigated." *Id.*

3. *Analysis*

Petitioner argues that claims 1–20 would have been obvious in view of Rockwood and Xie, offering two alternative mappings of the claims to the prior art. We find that neither is sufficient.

a. *Petitioner's "First Mapping"*

Independent claim 1 recites "gathering an event defining an action of *a first object acting on a target*, wherein the first object is executed on a device," and independent claims 10 and 17 similarly recite a sensor agent "operable to . . . gather an event defining an action of *a first object acting on a target*." Claims 1 and 10 also recite "correlating the event to *an originating object* of the first object," and claim 17 recites use of a

“contextual state” that “comprises an indication of *an originating object of the first object*.”

Petitioner’s first mapping is that “Rockwood discloses detecting and recording characteristics of a network event (corresponding to ‘gathering an event defining . . .’) including a source IP address (and its OS) of an event and a destination IP address (corresponding to ‘target’) for sent data (corresponding to ‘action . . .’).” Pet. 14–15 (citing Ex. 1004, 5:60–6:65, 13:45–65; Ex. 1002 ¶¶ 149–151). Petitioner further argues that “the device, operating as the source of the event and corresponding to the source IP address or source port, transmits data (of an event) *via the network layer / its operating system (OS) (corresponding to ‘first object’)*, which the system of Rockwood records in a detected event.” *Id.* at 15 (citing Ex. 1004, 6:25–35, 10:15–20, 12:25–55; Ex. 1002 ¶¶ 151–158) (emphasis added). Petitioner also asserts that one of skill in the art “would have understood that the network layer / OS (‘first object’) executes on a device (e.g., the device at the source IP).” *Id.* at 16 (citing Ex. 1002 ¶¶ 70–74, 149, 156).

So, in this first scenario, Petitioner is mapping the claim term “a first object” to the network layer or operating system of the device from which the detected event originated.⁴ We do not agree that the network layer or OS of the originating system could be “a first object” within the meaning of these claims. The claims require that the first object “act[] on a target,” and we fail to see how the network layer or operating system of the device from

⁴ Although Rockwood indicates that the system can detect the attacker’s operating system (*see, e.g.*, Ex. 1004, 12:39–41), it does not mention any “network layer.” That term appears to come from the Nielson Declaration. *See* Ex. 1002 ¶ 65–69.

which the detected event originated would be “acting on” the destination IP address, which is what Petitioner identifies as the “target.”

For the claimed “originating object of the first object,” Petitioner asserts that “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 information’) includes information such as originating processes, devices, and users.” Pet. 17 (citing Ex. 1002 ¶¶ 168–187; Ex. 1004, 2:60–3:5, 6:1–62, 13:1–24) (emphasis added). Petitioner argues that “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’).” *Id.* (citing Ex. 1002 ¶¶ 169–171; Ex. 1004, 7:60–8:5, 11:4–44, 12:36–55).

Here, however, Petitioner appears to map “originating object of the first object” to the “originating malware or source” or “the sources of attacks or originating malware,” rather than something that might have originated the network layer/OS, which is Petitioner’s “first object” in this mapping. This argument is thus unpersuasive because it is inconsistent with the analysis offered for the “first object” limitation. But even if we assume Petitioner intended to stay with the network layer/OS as the “first object,” it is unclear how or why the malware would be the “originating object” of the network layer or OS.

The “first object” and “originating object of the first object” mapping also presents a problem for the “correlating” limitations. Petitioner asserts that one of skill in the art “would have understood that Rockwood’s teachings of correlating events to sources of attacks using attacker profiles (which includes information relating to a device on which the first object (network layer / OS) is executed and a user associated with the first object) and attack attributes (e.g., target events) discloses ‘generating contextual state information.’” Pet. 18 (citing Ex. 1002 ¶¶ 176–179). The portions of Rockwood cited by Petitioner describe how the system correlates detected events with an attacker profile. *See* Ex. 1001, 7:60–8:5, 11:4–44, 12:36–55. But the claims require correlating the first object to an originating object of the first object, and, as explained above, it is unclear what might be the originating object of the network layer or operating system.

We also find it unclear which reference Petitioner relies on for the correlating. It appears that Petitioner finds the correlating in Rockwood (the reference with the attacker profile), but if Rockwood is intended to provide the correlating, it is unclear what role Xie has in the combination.

We further find that Petitioner does not adequately describe how these references might be combined. Rockwood describes a system that identifies attacks at a network edge as they occur,⁵ while Xie’s system looks for

⁵ Notably, the ’224 patent presents itself as an improvement over tools that “may reside at a network edge and may receive network events concerning the network from one or more hosts or systems” because “network edge devices have no ability to establish any sort of context from within the host or system that is generating the event.” Ex. 1001, 1:43–48. Rockwood appears to describe a network edge device. *See* Ex. 1004, 3:16–4:4 (“Each sensor 20 is located at a network port that receives TCP/IP packets or other similar network communications from network 100.”).

similar changes across different hosts within a network over multiple days. There is insufficient explanation of how Xie’s correlating technique would be beneficial in a system like that of Rockwood.

Finally, to the extent Petitioner intends to rely on Xie for correlating to an originating object, we find that reliance misplaced. Xie discloses a system that looks for corresponding changes over days across multiple hosts in a network to identify patterns that might be indicative of a problem. But Xie does not describe using correlation to identify an originating object. The correlation is between similar patterns across the network, meaning that, even when Xie identifies a correlation, it is not correlating an event to its originating object, but is merely identifying multiple close vectors (reflecting corresponding file changes) within a detection window. *See* Ex. 1005, 38. The system then identifies the involved hosts and files, which can be used by “system administrators [to] decide whether the updates are known administrative updates that should be suppressed, or some abnormal events that should be further investigated.” *Id.* at 39. Although Xie’s example used the “Lion” worm, the worm was known and introduced into the network for testing purposes, not identified by Xie’s system.

For these reasons, we find Petitioner’s first mapping insufficient to establish a reasonable likelihood that Petitioner can prove the challenged claims unpatentable in view of Rockwood and Xi.

b. Petitioner’s “Second Mapping”

In the alternative, Petitioner argues that “Rockwood also discloses detecting and recording characteristics of an event (corresponding to ‘gathering an event defining . . .’), including a transmitting source of an event and a destination IP address (corresponding to ‘target’) in which *the*

data/code package (corresponding to ‘first object’) is transmitted and executed on a network computer (corresponding to ‘executed on a device’).” Pet. 16 (citing Ex. 1004, 5:60–6:65, 12:35–45, 13:45–65; Ex. 1002 ¶¶ 158–160) (emphasis added). According to Petitioner, “Rockwood notes that the data package includes *executable code (corresponding to ‘first object’)* that may be malware; and, therefore, event attributes relating to the package (e.g., malware) transmission and its effect/action on a target (corresponding to ‘event defining an action . . .’) are collected by the system of Rockwood.” *Id.* (citing Ex. 1004, 3:50–60, 12:35–45; Ex. 1002 ¶¶ 159–163) (emphasis added).

This is a more appropriate mapping, as we agree that executable code could be an “object” within the scope of the claims. *See* Ex. 1001, 7:36–41 (“[a]n object . . . 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”). However, all claims require that the first object is “acting on a target,” and claim 1 requires that the first object is “executed on a device.” As Patent Owner argues (*see* Prelim. Resp. 42–44), although Rockwood identifies packages with executable code, it does not appear that the code in the packages is acting on a target or executed, and Petitioner does not adequately explain how that claim language is met in Rockwood. *See* Pet. 16–17. Petitioner does cite various passages of Rockwood, but we fail to see how the cited material supports an argument that Rockwood discloses a first object acting on a target or executed on a device. *See* Ex. 1004, 3:50–60 (explaining only that the sensors can use “any suitable detection technique to process and output detected events”), 5:60–6:65 (explaining that the sensors process packet headers, packet payloads, and/or other data),

12:35–45 (describing how the system detects events with “a segment of code” signifying that the event is an attack, but with no indication that the code acted on a target or was executed), 13:45–65 (describing how the system receives detected events and target events and assigns attribute values based on rules).

For his part, Mr. Nielson asserts that one of ordinary skill in the art would “recognize that . . . transmissions [of malware] are *intended* to execute transmitted malware on another device in the network in order to cause harm.” Ex. 1002 ¶ 163 (emphasis added). That may be true, but the fact that the sender *intends* for the malware to be executed is insufficient to show that the object is “acting on a target ” or “is executed on a device,” as the claim requires.

For the “correlating” in the second mapping, Petitioner asserts that “Rockwood and Xie disclose this limitation for the same reasons” as in the first mapping. Pet. 19. Petitioner contends that the “source of attack/originating object is the originating malware (‘originating object’)” and “the transmitted malware is the claimed first object.” *Id.* Petitioner asserts that the “process of correlating an event to an originating object (e.g., attacker profile with originating malware information as in Xie^[6]) that provides ‘contextual state information’ also applies to the above-referenced second mapping, and discloses this limitation.” *Id.* (citing Ex. 1002 ¶¶ 174–175, 177–187).

We find a number of problems with this analysis. First, Petitioner fails to explain how correlating an event to *an attacker profile* is sufficient to

⁶ It appears that Petitioner intends to refer to Rockwood here, as that is the reference with the attacker profile.

teach or suggest correlating an event to the “*the originating malware*,” which is what Petitioner has identified as the originating object of the first object in this mapping. Second, this mapping suffers from the problems identified above for the correlating in the first mapping: uncertainty about which reference is meant to provide the correlating, a lack of explanation of how these fundamentally different references might be combined, and the fact that Xie does not disclose correlating to an originating object.

For these reasons, we find Petitioner’s second mapping insufficient to establish a reasonable likelihood that Petitioner can prove the challenged claims unpatentable in view of Rockwood and Xi.

III. CONCLUSION

We determine that Petitioner has not shown a reasonable likelihood of proving that a challenged claim of the ’224 patent is unpatentable over Rockwood and Xi and, thus, do not institute an *inter partes* review.⁷

IV. ORDER

For the reasons given, it is ORDERED that no *inter partes* review is instituted in this proceeding.

⁷ Because we deny the Petition on the merits, we do not reach Patent Owner’s request that we exercise our discretion to deny the Petition based on the state of the related litigation. *See* Prelim. Resp. 3–20.

IPR2023-00657
Patent 10,257,224 B1

For PETITIONER:

Robert M. Hansen
Scott B. Amankwatia
Matthew J. Anderson
THE MARBURY LAW GROUP, PLLC
rhansen@marburylaw.com
samankwatia@marburylaw.com
manderson@marburylaw.com
pat-docketing@marburylaw.com

For PATENT OWNER:

Brian Eutermoser
Russell E. Blythe
Mikaela Stone
KING & SPALDING LLP
beutermoser@kslaw.com
rblythe@kslaw.com
mikaela.stone@kslaw.com