

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

TREND MICRO, INC.,  
Petitioner,

v.

OPEN TEXT INC.,  
Patent Owner.

---

IPR2023-00677  
Patent 9,578,045 B2

---

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

WORMMEESTER, *Administrative Patent Judge*.

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

## I. INTRODUCTION

Trend Micro, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–19 of U.S. Patent No. 9,578,045 B2 (Ex. 1001, “the ’045 patent”). Open Text Inc. (“Patent Owner”)<sup>1</sup> filed a Preliminary Response (Paper 6, “Prelim. Resp.”). Under 35 U.S.C. § 314(a), 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.” See 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”). For the reasons that follow, we decline to institute an *inter partes* review.

## II. BACKGROUND

### A. Related Proceedings

The parties identify four federal district court cases, one of which involves Petitioner as a defendant. Pet. 1–2; Paper 4, 1 (Patent Owner’s mandatory notices). Patent Owner also identifies several *inter partes* review proceedings. Paper 4, 1–3. One of the proceedings, IPR2023-00124, involves the ’045 patent. Two other proceedings, IPR2023-00126 and IPR2023-00657, involve U.S. Patent No. 10,257,224, which Patent Owner asserts “is related to the ’045 Patent.” *Id.* at 3. According to Patent Owner, the remaining proceedings are “not related to the ’045 Patent,” but they are “also asserted in the related district court litigations.” *Id.* at 2–3.

---

<sup>1</sup> The Petition’s caption identifies Webroot Inc. as the patent owner. In Patent Owner’s mandatory notices, however, Patent Owner identifies itself, Open Text Inc., as the patent owner “due to a change in ownership of U.S. Pat. No. 9,578,045.” Paper 4, 1 n.1.

*B. The '045 Patent*

The '045 patent describes “forensic visibility into client systems having full audit trails.” Ex. 1001, 1:15–18. The '045 patent explains that “existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic,” including hostnames, ports, protocols, and IP addresses. *Id.* at 1:34–39. The '045 patent refers to such tools as network edge devices. *Id.* at 1:52–56. According to the '045 patent, network edge devices “tend to receive network events outside of a host or system,” with “no ability to establish any sort of context from within the host or system that is generating the event.” *Id.* at 1:39–46. That is, a network edge device “may monitor, record, and . . . analyze network traffic between the host and the device, but information that may be useful within the host is not obtained.” *Id.* at 1:46–49. Thus, “[a] network edge device . . . has no way of knowing to what extent [a] virus may have impacted [a] computing device . . . , what additional files may have become infected, or what processes and/or objects operating are linked to the virus.” *Id.* at 2:12–16.

As a solution, the '045 patent proposes “a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event.” Ex. 1001, 2:23–27. The '045 patent describes in particular “a sensor agent [that] 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 2:27–31. In one embodiment, “[a] computing device 204 includes and/or executes a sensor agent 208 in

connection with the presentation of content to the user.” *Id.* at 7:9–11. Sensor agent 208 uses various components to gather and process events, including system filter 340, local aggregator and interpreter 344, context analyzer 348, global perspective unit 352, event distributor 356, and event priority generation unit 358. *Id.* at 7:11–17, Figs. 2, 3.

Figure 6 of the ’045 patent is reproduced below.

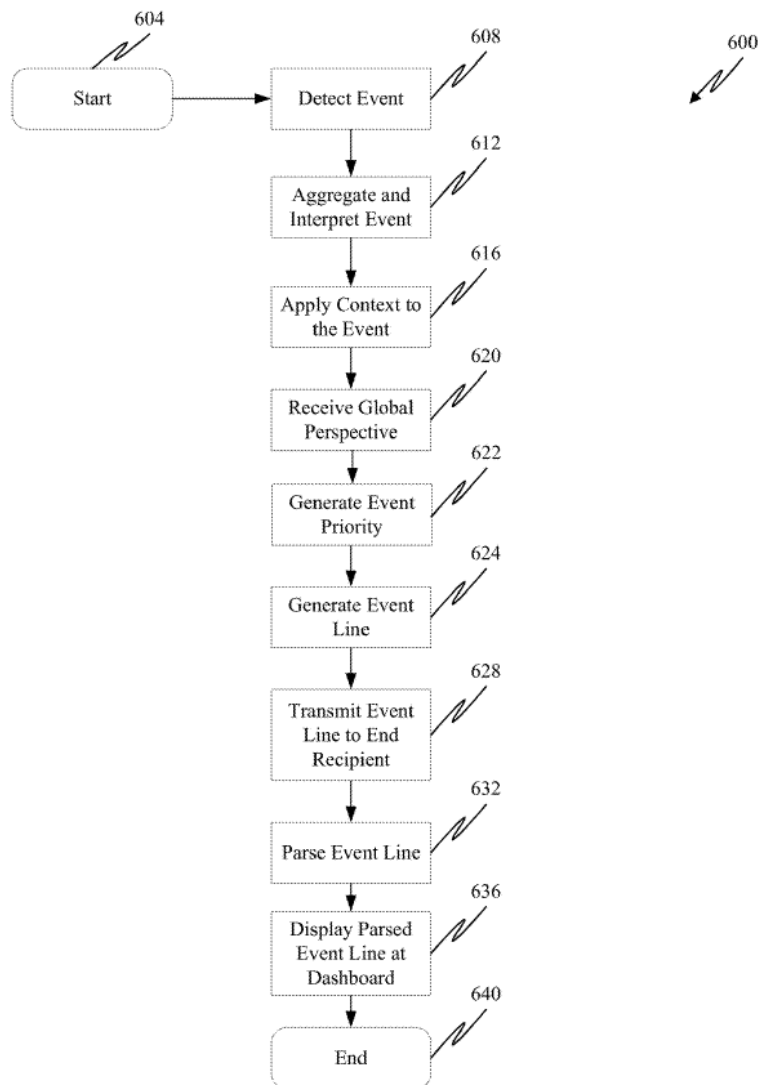


Figure 6

Figure 6 illustrates a method that sensor agent 208 may perform for providing forensic visibility into a system. Ex. 1001, 6:16–18, 18:3–7.

Method 600 starts at step 604, where events of computing system 204 are initiated. *Id.* at 18:19–21. These events are detected at step 608 by the sensor agent’s system filter 340. *Id.* at 18:21–24. At step 612, the sensor agent’s local aggregator and interpreter 344 receives the events from system filter 340. *Id.* at 18:44–47. At step 616, “a contextual state may be applied by [the sensor agent’s] context analyzer 348 to the event information,” where context analyzer 348 correlates events to objects so that an audit trail for each event is created. *Id.* at 18:53–55.

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, 18:61–63. 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 18:64–19:5.

At step 622, “an event priority may be applied to the event,” where “the event priority may be obtained . . . [by] applying . . . a rule set to aggregated event information, contextual state information, and global perspective information.” Ex. 1001, 19:5–10. At step 624, “such data is appended to each relevant portion of an event line.” *Id.* at 19:10–12. At step 628, the sensor agent’s “event distributor 356 may transmit the event line 244 to the end recipient 220.” *Id.* at 19:13–15.

At recipient 220, the event line is parsed at step 632 to filter out one or more events, and the parsed event line is then displayed on a dashboard at step 636. Ex. 1001, 19:17–22. Method 600 ends at step 640. *Id.* at 19:22.

*C. Illustrative Claim*

As noted above, Petitioner challenges claims 1–19 of the '045 patent, where claims 1, 8, and 16 are independent. Claim 1, reproduced below, is illustrative of the claims under challenge.

1. A method comprising:

gathering one or more events defining an action of a first object acting on a target;

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object 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;

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, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;

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; and

transmitting the assembled event line.

*D. Asserted Ground of Unpatentability*

Petitioner challenges claims 1–19 of the '045 patent on the following sole ground. Pet. 4, 10–66.

| Claims Challenged | 35 U.S.C. §      | References/Basis                        |
|-------------------|------------------|-----------------------------------------|
| 1–19              | 103 <sup>2</sup> | Rockwood, <sup>3</sup> Xie <sup>4</sup> |

In support of its challenge, Petitioner relies on a declaration of Dr. Seth Nielson, Ph.D. (Ex. 1002). Patent Owner relies on a declaration of Dr. Nenad Medvidovic, Ph.D. (Ex. 2001) to support its response.

### III. DISCUSSION

#### *A. Claim Construction*

In an *inter partes* review proceeding, we construe a claim of a patent “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” *See* 37 C.F.R. § 42.100(b). That standard involves construing claims in accordance with the ordinary and customary meaning of such claims as would have been understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc).

Petitioner asserts that, “[i]n parallel litigation, [Patent Owner] argues all claim terms should be given their plain and ordinary meanings, except for [the claim term] ‘wherein the global perspective for one or more related events to the at least one event across a network’” for which Patent Owner

---

<sup>2</sup> The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the application from which the ’045 patent issued was filed after this date, the AIA version of § 103 applies.

<sup>3</sup> Rockwood, U.S. Patent No. 7,352,280 B1, issued Apr. 1, 2008 (Ex. 1004).

<sup>4</sup> Yinglian Xie, A Spatiotemporal Event Correlation Approach to Computer Security (Aug. 2005) (Ph.D. thesis, Carnegie Mellon University) (Ex. 1005).

proposes a construction. Pet. 9. Petitioner further asserts that, “[f]or purposes of this proceeding only, Petitioner proposes the Board adopt [Patent Owner]’s proposals.” *Id.*

Patent Owner does not respond other than to assert that the district court has provided various claim constructions. Prelim. Resp. 23–26. Patent Owner asserts that it “appl[ies] the Court’s construction for all construed terms and the plain and ordinary meaning of the claim terms that the Court did not construe.” *Id.* at 26.

On the record before us, we conclude that no claim term requires express interpretation to resolve any controversy in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

### *B. Obviousness over Rockwood and Xie*

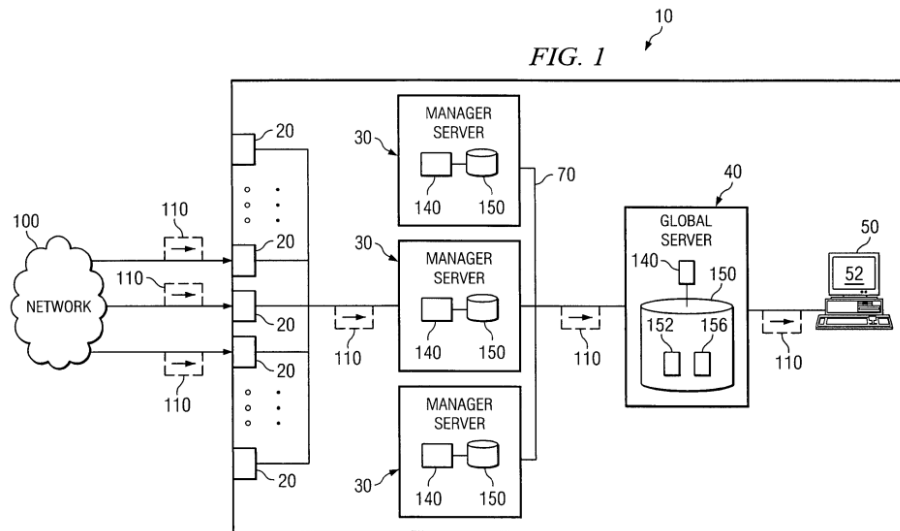
Petitioner asserts that claims 1–19 of the ’045 patent would have been obvious over Rockwood and Xie. Pet. 4, 10–66. Patent Owner challenges certain aspects of Petitioner’s analysis. Prelim. Resp. 34–68. For the reasons explained below, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on its asserted ground.

Before addressing the parties’ arguments, we provide an overview of the asserted references, Rockwood and Xie.

#### *1. Overview of Rockwood*

Rockwood describes “intrusion detection systems . . . for intruder tracking using advanced correlation in a network security system.”

Ex. 1004, 1:8–11. Figure 1 of Rockwood, reproduced below, illustrates an example intrusion detection system.



In particular, Figure 1 of Rockwood shows intrusion detection system 10, which is distributed across an enterprise system. *Id.* at 2:38–40. System 10 includes sensors 20, manager servers 30, global server 40, and console 50. *Id.* at 2:40–43. These system elements may communicate with each other through internal network 70. *Id.* at 2:43–44.

Figure 2 of Rockwood is reproduced below.

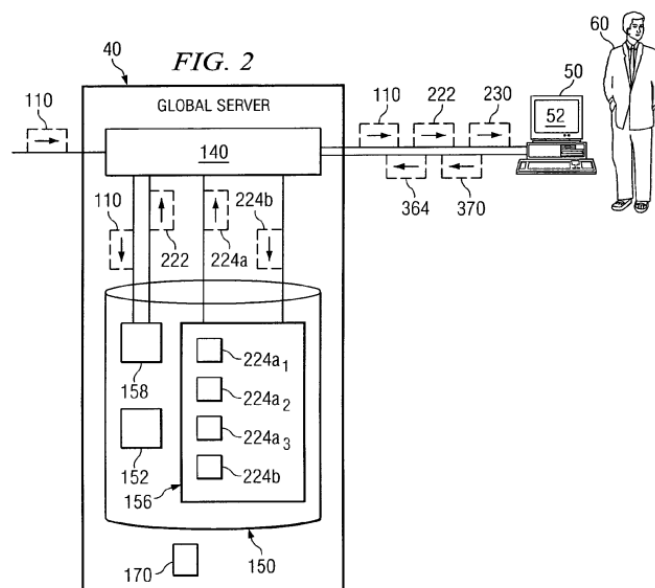


Figure 2 of Rockwood shows the flow of operation of elements in system 10. *Id.* at 5:60–61. Global server 40 receives detected events 110 from manager servers 30, where each detected event 110 includes attributes (or characteristics) 410 such as time, source IP address, and destination IP address. *Id.* at 5:61–66. Correlation engine 140 uses rules in ruleset 152 to process each detected event 110 by assigning attribute values 420 to the detected event according to particular attributes 410 of the detected event. *Id.* at 6:1–9. To further illustrate, Figure 3 of Rockwood is reproduced below.

**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              |                 |

Figure 3 of Rockwood is a table of event information. *Id.* at 2:15–16. As can be seen, one attribute 410a of each detected event is time. *Id.* at 6:13–14. Detected event 110a in particular has attribute 410a of 5:25 pm. *Id.* Ruleset 152 has a rule to assign to each detected event an attribute value equal to the decimal time of that detected event. *Id.* at 6:16–18. Thus, correlation engine 140 assigns to detected event 110a attribute value 420a of 17.42, which is the decimal form of 5:25 pm. *Id.* at 6:18–21. Correlation engine 140 stores each detected event in detected event storage 158 according to attribute values 420 of that detected event. *Id.* at 6:35–38.

Rockwood explains that “correlation engine 140 is operable to correlate detected events 110 in detected event storage 158 to detect an attack occurring upon or within the enterprise,” and “is further operable to

determine the likely identity of an attacker.” Ex. 1004, 6:63–67. With respect to detecting an attack on the enterprise, Rockwood teaches correlating detected events 110 using target event 364 and proximity limits 370. *Id.* at 6:67–7:3. For example, operator 60 may learn from an external source that an attack on internal network 70 occurred at 5:20 pm from source IP address 205.252.48.166. *Id.* at 8:55–57. To determine whether any detected events in storage 158 are similar to the attack, operator 60 inputs the attack into console 50 as target event 364. *Id.* at 8:57–61. Console 50 then sends target event 364 to global server 40, where correlation engine 140 assigns attribute values to target event 364 based on rules in ruleset 152. *Id.* at 8:64–9:3, Fig. 3. In this example, operator 60 defines similar attacks as detected events 110 originating within forty-five minutes and twenty IP address units of target event 364. *Id.* at 9:4–7. Operator 60 inputs proximity limit 370a of forty-five minutes and proximity limit 370b of twenty address units into console 50, which sends the limits to global server 40, where correlation engine 140 assigns respective attribute values 420 (e.g., attribute value 420a of 0.75 and attribute value 420b of 20) based on rules in ruleset 152. *Id.* at 9:7–16, Fig. 3.

Figure 4 of Rockwood is reproduced below.

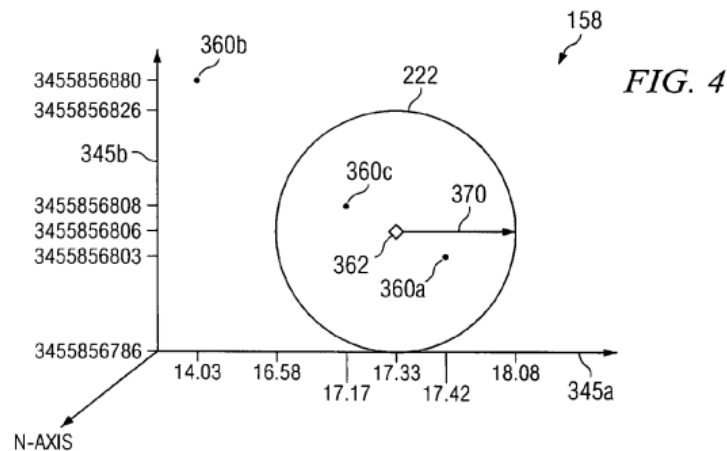


Figure 4 shows stored event information. Ex. 1004, 2:17–18. Axis 345a represents attribute value 420a of decimal time, and axis 345b represents attribute value 420b of base ten source IP address. *Id.* at 9:31–34. Attribute values 420 of target event 364 define target point 362 in n-dimensional space at coordinates 17.33 and 3455856806. *Id.* at 9:41–43. Similarly, attribute values 420 of detected event 110a define point 360a, attribute values 420 of detected event 110b define point 360b, and attribute values 420 of event 110c define point 360c. *Id.* at 9:34–41. Proximity limits 370 (e.g., 0.75 decimal time and 20 IP address units) define a portion of n-dimensional space surrounding target point 362. *Id.* at 9:47–49. Correlation engine 140 identifies points 360a and 360c, which correspond respectively to detected events 110a and 110c, as within proximity limits 370 of target point 362. *Id.* at 9:49–59. In other words, detected events 110a and 110c are “similar to the attack.” *See id.* at 9:62–67. Global server 40 sends detected events 110a and 110c as identified detected events 222 to console 50, which displays identified detected events 222 to operator 60. *Id.* at 9:59–62. According to Rockwood, “[b]y identifying detected events 110 that are similar to the attack represented by target event 364, operator 60 may be better able to prevent future attacks.” *Id.* at 9:64–67.

With respect to determining the likely identity of an attacker, Rockwood teaches correlating identified detected events 222 with attacker profiles 224a stored in profile set 156. Ex. 1004, 10:1–4. Each attacker profile 224a includes characteristics of an attacker of an enterprise. *Id.* at 10:8–11. For example, attacker profile 224a may correspond to an individual who normally launches attacks between 5:00 pm and 5:30 pm

using external computers with IP addresses between 205.252.48.160 and 205.252.48.200. *Id.* at 10:14–19. If identified detected events 222 do not correlate with any existing attacker profile 224a, correlation engine 140 generates new attacker profile 224b based on the event information of identified detected events 222. *Id.* at 10:4–8. Rockwood explains that “[b]y determining the identity of an attacker, operator 60 may be able to preempt future attacks.” *Id.* at 10:20–22.

## 2. Overview 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.<sup>5</sup> 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,” where “[t]he correlation is performed by clustering points, each representing an individual host state transition, in a multi-dimensional feature space.” *Id.*

The thesis explains that “[m]any attacks install new files on a compromised host, or modify files that are infrequently updated,” and, therefore, “[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. Xie’s system generates vectors corresponding to host file updates over a one-day detection window and then correlates those vectors with vectors

---

<sup>5</sup> Citations to Xie refer to the exhibit page numbers added by Petitioner.

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.* Xie explains that "[t]he 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 of Claims 1–19*

We turn now to the claims. Petitioner offers two alternative mappings of the claims to the asserted prior art. As discussed below, we find that neither is sufficient.

#### *a. Petitioner's First Mapping*

Independent claim 1 recites "gathering one or more events defining an action of *a first object acting on a target*," and independent claims 8 and 16 similarly recite "operable to[] gather one or more events defining an action of *a first object acting on a target*" (emphases added). The claims also recite "generating a contextual state . . . 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*” (emphases added).<sup>6</sup> Ex. 1001, claim 1; *id.* at claims 8, 16 (reciting “generate” instead of “generating”). We address these limitations.

*i. “first object acting on a target”*

Under what Petitioner calls its “first mapping,” Petitioner asserts that “Rockwood discloses detecting and recording characteristics of a network event (corresponding to ‘gathering one or more events defining . . .’) including a source IP address (and its OS [operating system]) of an event and a destination IP address (corresponding to ‘target’) for sent data (corresponding to ‘action . . .’).” Pet. 14 (citing Ex. 1004, 5:60–6:65, 13:45–65; Ex. 1002 ¶¶ 149–151). Petitioner further asserts 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 14–15 (emphasis added) (citing Ex. 1004, 6:25–35, 10:15–20, 12:25–55; Ex. 1002 ¶¶ 149–153). Petitioner also asserts that an ordinarily skilled artisan “would have understood that the network layer/OS (‘first object’) executes on a device (e.g., the device at the source IP).” *Id.* at 15–16 (citing Ex. 1002 ¶¶ 63–85, 143–152).

Here, Petitioner is mapping the claim term “a first object” to the network layer or operating system of the device from which the detected

---

<sup>6</sup> We treat the claim term “an originating object” as providing antecedent basis for the claim term “the originating object of the first object,” and, therefore, we treat the two terms as the same.

event originated.<sup>7</sup> We are not persuaded that the network layer or operating system of the originating system could be “a first object” within the meaning of the claims of the ’045 patent. 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 which the detected event originated would be “acting on” the destination IP address, which is what Petitioner identifies as the “target.”

*ii. “originating object of the first object”*

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’) includes information such as originating processes/objects, devices, and users.” Pet. 17 (emphasis added) (citing Ex. 1002 ¶¶ 166–170; Ex. 1004, 2:60–3:5, 6:1–62, 13:1–24). Petitioner further asserts 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

---

<sup>7</sup> Although Rockwood indicates that the system can detect the attacker’s operating system (*see, e.g.,* Ex. 1004, 12:39–41), Rockwood does not mention any “network layer.” That term appears to come from Dr. Nielson’s declaration testimony. *See* Ex. 1002 ¶¶ 66–70.

an attacker profile or originating malware (‘originating object’).” *Id.* (citing Ex. 1002 ¶¶ 166–171; Ex. 1004, 7:60–8:5, 11:4–44, 12:36–55).

Patent Owner responds that “the claims of the ’045 patent describe the ‘first object’ as an object that is ‘originated’ by another object,” and that “Petitioner does not identify any disclosure in Rockwood (or anywhere else) that discloses or explains how an operating system or network layer is originated by another object.” Prelim. Resp. 42–43. Patent Owner contends that “Petitioner asserts that Rockwood’s ‘source[] of attack[] or originating malware’ is the claimed ‘originating object,’” yet “under Petitioner’s theory, to comport with the ’045 claims, the ‘source[] of attack[] or originating malware’ would have to *originate* a computer’s network layer or operating system, which is unsupported and nonsensical.” *Id.* at 43. According to Patent Owner, “[m]alware is not the originating object of a network layer or operating system.” *Id.*

We agree with Patent Owner. 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. *See* Pet. 17. Petitioner’s showing is thus unpersuasive because it is inconsistent with the analysis offered for the “first object” limitation. Even if we were to 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.

*iii. Other Deficiencies*

The “first object” and “originating object of the first object” mapping also presents a problem for the “correlating” limitations. Petitioner asserts that an ordinarily skilled artisan “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 a contextual state.’” Pet. 18 (citing Ex. 1002 ¶¶ 174–177). The portions of Rockwood cited by Petitioner describe how the system correlates detected events with an attacker profile. *See* Ex. 1004, 7:60–8:5, 11:4–44, 12:36–55. The claims, however, require correlating to an originating object (i.e., the 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 additionally 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 Petitioner’s proposed combination. *See* Pet. 17–18.

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,<sup>8</sup> whereas Xie’s system looks for 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 uses the “Lion” worm, as Petitioner points out (*see* Pet. 18), the worm was known and introduced into the network for testing purposes, not identified by Xie’s system (*see* Ex. 1005, 47–48).

---

<sup>8</sup> Notably, the ’045 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, 1:40–46. 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.”).

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 Xie.

*b. Petitioner’s Second Mapping*

As discussed above, the claims require gathering one or more events defining an action of *a first object acting on a target*, as well as generating a contextual state by correlating the one or more events to *an originating object*, where the contextual state includes an indication of the *originating object of the first object*. Petitioner’s alternative showing for these limitations also is insufficient.

*i. “first object acting on a target”*

Under what Petitioner calls its “second mapping,” Petitioner asserts that “Rockwood also discloses detecting and recording characteristics of an event (corresponding to ‘gathering one or more events defining . . .’), including a transmitting source of an event and a destination IP address (corresponding to ‘target’) where *the data/code package (corresponding to ‘first object’)* is transmitted.” Pet. 16 (emphasis added) (citing Ex. 1004, 5:60–6:65, 12:35–45, 13:45–65; Ex. 1002 ¶¶ 153–160). 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 ‘events defining an action of the first object . . .’) are collected by the system of Rockwood.” *Id.* (emphasis added) (citing Ex. 1004, 3:50–60, 12:35–45; Ex. 1002 ¶¶ 153–160).

Patent Owner responds that “Rockwood does not disclose any computer object that is ‘acting’ on a target.” Prelim. Resp. 45. Patent Owner asserts that “[t]he ’045 patent describes the claimed ‘action’ on a target as an event type, such as a registry edit, that has been performed on a target.” *Id.* at 45–46 (citing Ex. 1001, 17:20–29). According to Patent Owner, “Petitioner’s claim that Rockwood discloses transmitting a data package that ‘may be malware’ does not define a first object ‘acting’ on a target.” *Id.* at 46.

We agree with Patent Owner. Petitioner’s alternative theory provides a more appropriate mapping, as we agree that the executable code could be an “object” within the scope of the claims. *See* Ex. 1001, 7:32–36 (“An 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, the claims require that the first object is “acting on a target.” As Patent Owner argues (*see* Prelim. Resp. 45–49), although Rockwood identifies packages with executable code, it does not appear that the code in the packages is acting on a target, and Petitioner does not adequately explain how the claim language is met in Rockwood. *See* Pet. 16. 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. *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 each detected event includes a plurality of characteristics or attributes, such as time, source IP address, and destination IP address), 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), 13:45–65 (describing how the system receives detected events and target events and assigns attribute values based on rules); *see also* Prelim. Resp. 47–48 (discussing portions of Rockwood cited by Petitioner).

*ii. Other Deficiencies*

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 further asserts that the “source of attack/originating object is the originating malware (‘originating object’)” and that “the transmitted malware is the claimed first object.” *Id.* Additionally, Petitioner asserts that the “process of correlating an event to an originating object (e.g., attacker profile with originating malware information as in Xie[<sup>9</sup>]) that provides ‘contextual state’ also applies to the above-referenced second mapping and discloses this limitation.” *Id.* (citing Ex. 1002 ¶¶ 171–173).

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 teach or suggest correlating an event to 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

---

<sup>9</sup> It appears that Petitioner intends to refer to Rockwood here, as that is the reference with the attacker profile.

that Xie does not disclose correlating to an originating object. *See supra* Part III.B.3.a.

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 Xie.

#### 4. Summary

In view of the foregoing, we determine that Petitioner has not demonstrated a reasonable likelihood of showing that independent claims 1, 8, and 16 would have been obvious over Rockwood and Xie. Claims 2–7, 9–15, and 17–19 depend from claims 1, 8, or 16. Accordingly, we also determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on its assertion as to these dependent claims.

### IV. CONCLUSION

For the foregoing reasons, Petitioner has not demonstrated on the record before us a reasonable likelihood that it would prevail in showing the unpatentability of any of the challenged claims of the '045 patent. Therefore, we do not institute trial.<sup>10</sup>

### V. ORDER

For the reasons given, it is

ORDERED that the Petition is *denied* and no trial is instituted.

---

<sup>10</sup> 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. 2–19.

IPR2023-00677  
Patent 9,578,045 B2

For PETITIONER:

Robert M. Hansen  
Scott B. Amankwatia  
Matthew J. Anderson  
THE MARBURY LAW GROUP, PLLC  
bhansen@marburylaw.com  
samankwatia@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