

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

IPR2025-00070
Patent 9,954,872 B2

Before NEIL T. POWELL, STACEY G. WHITE, and GARTH D. BAER,
Administrative Patent Judges.

POWELL, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. BACKGROUND

CrowdStrike, Inc. (“Petitioner”) filed a Petition for *inter partes* review of claims 1–21 of U.S. Patent No. 9,954,872 B2 (Ex. 1001, “the ’872 patent”). Paper 1 (“Pet.”). GoSecure, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). We authorized Petitioner to file a Preliminary Reply and Patent Owner to file a Preliminary Sur-Reply. Paper 9 (“Prelim. Reply”); Paper 10 (“Prelim. Sur-Reply”).

We instituted *inter partes* review. Paper 15 (“Initial Institution Decision” or “Init. Inst. Dec.”). After our Initial Institution Decision was vacated (Paper 25), we again instituted *inter partes* review. Paper 28 (“Second Institution Decision” or “2d Inst. Dec.”). During trial, Patent Owner filed a Response to the Petition (Paper 47, “PO Resp.”), Petitioner filed a Reply (Paper 50, “Reply”), and Patent Owner filed a Sur-reply (Paper 54, “Sur-Reply”).

We held an oral hearing in this proceeding on June 10, 2026, and a copy of the transcript is entered into the record. Paper 61 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6, and this Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during the review. For the reasons discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claims 1, 3–7, and 9–21 of the ’872 patent are unpatentable, but has not shown that claims 2 and 8 are unpatentable.

B. REAL PARTIES IN INTEREST

Petitioner identifies CrowdStrike, Inc. and CrowdStrike Holdings, Inc. as the real parties-in-interest. Pet. 77. Patent Owner identifies GoSecure, Inc. as the real party-in-interest. Paper 11, 1.

C. RELATED PROCEEDINGS

The parties note that the '872 patent is involved in *GoSecure Inc. v. CrowdStrike, Inc., and CrowdStrike Holdings, Inc.*, Case No. 24-cv-526 in the Western District of Texas, Austin Division. Pet. 77; Paper 5, 1. Additionally, Petitioner notes that it filed another petition challenging claims of the '872 patent in IPR2025-00068.¹ Pet. 77.

D. THE '872 PATENT

The '872 patent “relates generally to systems and methods for protecting computer networks, including but not limited to systems and methods for analyzing malicious activities on a computer system in order to better protect the computer from future malicious activity.” Ex. 1001, 1:44–48. The '872 patent discusses more details in connection with Figure 1, which is reproduced below.

¹ Institution of *inter partes* review has been denied in IPR2025-00068. IPR2025-00068, Paper 28.

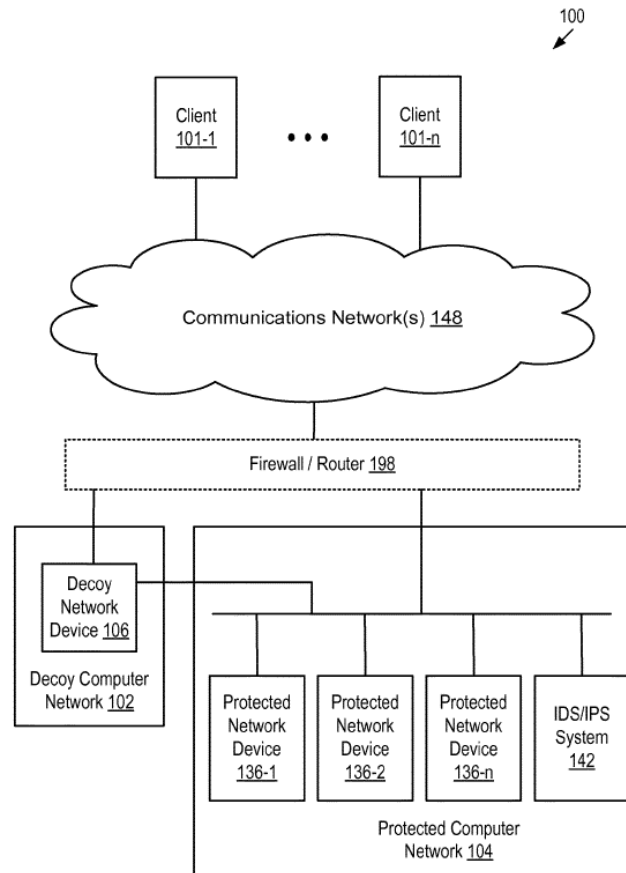


Figure 1

The '872 patent explains that “[Figure] 1 is a high-level block diagram illustrating an exemplary distributed computer system.” Ex. 1001, 3:26–28.

More specifically, Figure 1 shows distributed computer system 100, which “includes a decoy computer network 102, a communications network 148, and protected computer network 104.” Ex. 1001, 4:5–8. Additionally, client computers 101 may have access to decoy computer network 102 and protected computer network 104 via communications network 148. *Id.* at 4:13–24.

“Typically, the protected computer network 104 includes a firewall/router 198 to protect the protected network devices 136 and route network traffic to and from the protected network devices 136.” Ex. 1001, 4:30–33. “In some embodiments, the protected computer

network 104 also includes an IDS/IPS system 142 (intrusion detection and prevention system).” *Id.* at 4:37–39. IDS/IPS system 142 may use “fingerprints of unauthorized activities” to “prevent[] unauthorized activities matching the stored fingerprints by modifying the protected network devices 136 and/or the firewall/router 198.” *Id.* at 4:39–47.

“The decoy computer network 102 includes one more decoy network device(s) 106. The decoy network device 106 is a decoy system that is monitored to collect fingerprint data of unauthorized activities.”

Ex. 1001, 4:57–60. “In some embodiments, the decoy network device 106 is intentionally kept vulnerable to unauthorized or malicious activities (e.g., known security weaknesses may be intentionally left unfixed or other security components (e.g., firewalls) are intentionally not installed).”

Id. at 4:60–65. “The purpose of the decoy network device 106 is to allow attackers to attack the decoy network device 106, so that the pattern of attack can be monitored and analyzed to generate a fingerprint,” which can be used to forestall similar future attacks. *Id.* at 5:3–9. Along with other components, decoy network device 106 may include at least one virtual machine. *Id.* at 5:31–32, 59–61, 6:6–9, 6:24–28, Fig. 2.

The ’872 patent discusses a method that decoy network device 106 may perform in connection with Figures 6A–6C, which are reproduced below.

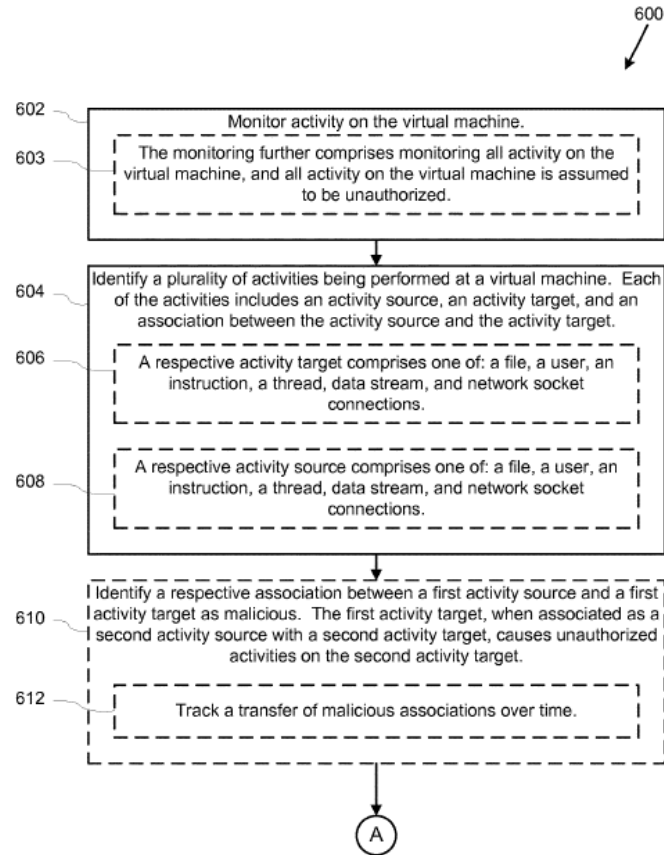


Figure 6A

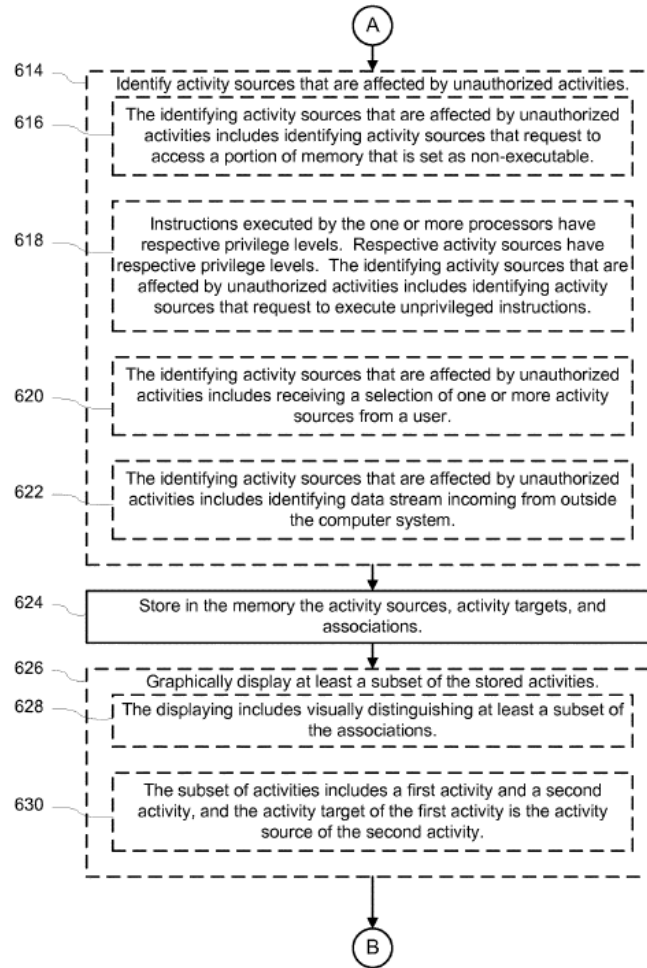


Figure 6B

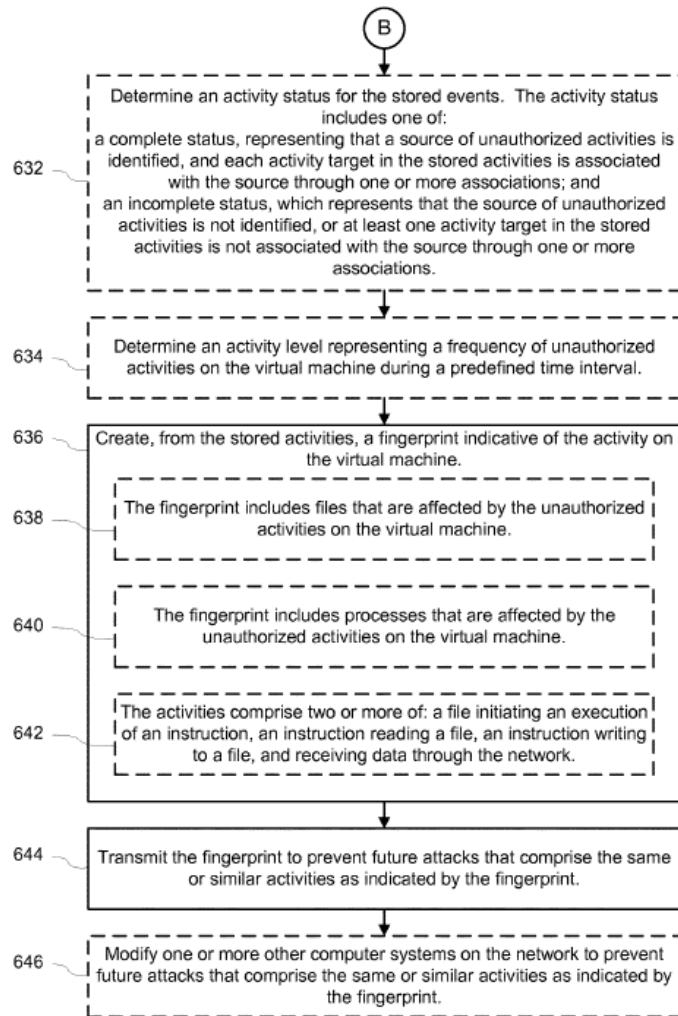


Figure 6C

The '872 patent explains that “[Figures] 6A-6C are flowcharts representing a method of identifying unauthorized activities on a computer system.”

Ex. 1001, 3:47–49.

In this method, “[t]he decoy network device monitors (602) activity on the virtual machine.” Ex. 1001, 15:7–8. Additionally, “[t]he decoy network device identifies (604) a plurality of activities being performed at the virtual machine.” *Id.* at 15:25–26. “In some embodiments, the decoy network device identifies (610) a respective association between a first activity source and a first activity target as unauthorized.” *Id.* at 15:48–50.

Later, “[t]he decoy network device stores (624) the activity sources, activity targets, and associations in its memory.” *Id.* at 16:56–57. The decoy network device also “creates (636) a fingerprint indicative of the activity on the virtual machine from the stored activities.” *Id.* at 18:4–6. The decoy network device may share the fingerprint:

The decoy network device transmits (644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the decoy network device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.

In some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in FIG. 1A, the IDS/IPS system modifies at least one of the protected network device(s) 136 to prevent future attacks that comprise the same or similar activities).

Ex. 1001, 18:44–58.

E. ILLUSTRATIVE CLAIMS

Of the challenged claims, claims 1, 20, and 21 are independent. Each of claims 2–19 depends, directly or indirectly, from independent claim 1. Claim 1 is illustrative for our analysis herein and is reproduced below with certain reformatting:²

1. [1(pre)] A computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, the method comprising:
[1(a)] monitoring activity on the first computer system;

² We have added the same labels that Petitioner uses to identify portions of claim 1. *See, e.g.*, Pet. 80.

- [1(b)] identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
- [1(c)] storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and
- [1(d)] transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:39–59.

F. ASSERTED GROUNDS

Petitioner asserts that claims 1–21 are unpatentable on the following grounds (Pet. 9):

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1–6, 12, 15, 20, 21	103	Capalik ³
2	1–6, 12, 14, 15, 20, 21	103	Capalik, Goel ⁴
3	7–11, 14, 16, 18, 19	103	Capalik, Goel, King ⁵

³ Alen Capalik, United States Patent Application Publication No. 2008/0016570 A1, published Jan. 17, 2008 (Ex. 1004, “Capalik”).

⁴ Ashvin Goel et al. “*Forensix: A Robust, High-Performance Reconstruction System*,” Proceedings of the 25th International Conference on Distributed Computing Systems Workshops, 2005 (Ex. 1005, “Goel”).

⁵ Samuel T. King, “*Analyzing Intrusions Using Operating System Level Information Flow*” 2006 (Ex. 1006, “King”).

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
4	13	103	Capalik, Goel, Pike ⁶
5	17	103	Capalik, Goel, Farley ⁷

In support of its challenges, Petitioner also relies on the declarations of Markus Jakobsson, Ph.D. Ex. 1003 (“first declaration”); Ex. 1035 (“supplemental declaration”). Patent Owner relies on a declaration of Angelos Stavrou, Ph.D. Ex. 2031.

II. PROCEDURAL DISPUTE REGARDING LIMITATION 1(D)

After Patent Owner filed its Preliminary Response, with our authorization, Petitioner filed its Preliminary Reply, and Patent Owner filed its Preliminary Sur-Reply. In its Response, Patent Owner argues that Petitioner’s Preliminary Reply raised procedurally improper arguments that were not presented in the Petition. PO Resp. 23–24. Specifically, Patent Owner argues that Petitioner “changed its theory of unpatentability by arguing that the ‘other’ ‘computer systems’ recited in claim 1 are taught by ‘the protected network, including protected endpoint devices and the IDS/IPS.’” *Id.* at 23 (citing Prelim. Reply 2). Patent Owner asserts that “[t]he Board should not consider [Petitioner’s] new theory, which is not in the Petition.” *Id.* at 24.

Petitioner counters that (1) “[t]he Petition mapped Capalik’s transmission to the IDS/IPS *as a component of* protected network 504 and explained that the *purpose* was to protect the devices within the protected

⁶ Geoffrey Pike et al., U.S. Patent No. 8,819,822 B1, issued Aug. 26, 2014 (Ex. 1007, “Pike”).

⁷ Timothy P. Farley et al., U.S. Patent No. 7,089,428 B2, issued Aug. 8, 2006 (Ex. 1008, “Farley”).

network 504” and (2) petitioners may respond to patent owner arguments by clarifying or elaborating on its arguments. Reply 11.

We agree with Petitioner that the Petition’s arguments sufficiently convey that Capalik teaches limitation 1(d) by sending an attack signature to protected computer network 504, specifically to protected computer network 504’s IDS/IPS library. *See, e.g.*, Pet. 34 (“A POSITA would have further understood that *Capalik* transmits this information to a computer system other than computer decoy 502 since the signature is sent ‘through a standard network connection’ to IDS/IPS 534 ***of protected network 504.***” (emphasis added)). Thus, Petitioner’s Preliminary Reply arguments are merely clarifying and elaborating on the Petition’s position. Accordingly, we decline Patent Owner’s request that we not consider Petitioner’s position.

III. ANALYSIS

A. LEVEL OF ORDINARY SKILL

Petitioner explains the applicable level of skill in the art as follows:

As of June 24, 2010, a person of ordinary skill in the art (POSITA) would be a person having a bachelor’s degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and who would have had a working knowledge of software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

Pet. 8 (Ex. 1003 ¶¶ 30–31). Patent Owner does not dispute Petitioner’s explanation of the level of skill in the art. *See* Ex. 2031 ¶¶ 15–16.

We adopt Petitioner’s uncontested proposed level of ordinary skill in the art, which we find consistent with the level of ordinary skill in the art reflected by the ’872 patent and the prior art of record. *See Okajima v.*

Bourdeau, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

B. CLAIM CONSTRUCTION

In an *inter partes* review, we apply the same claim construction standard as would be used by a district court to construe a claim in a civil action involving the validity or infringement of a patent. 37 C.F.R. § 42.100(b). Under that standard, claim terms are given their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history of record. *Id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–19 (Fed. Cir. 2005) (en banc); *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365–66 (Fed. Cir. 2012).

Additionally, only terms that are in controversy need to be construed, and these terms need be construed only to the extent necessary to resolve the controversy. *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)). In order to resolve the parties’ patentability disputes, we need only resolve claim-construction issues for limitation 1(d), claim 2, and claim 8.

1. Limitation 1(d)

Limitation 1(d) recites transmitting information for preventing future attacks:

transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems,

associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:53–59. The same requirement is recited in each of limitations 20(d) and 21(d) of independent claims 20 and 21, respectively. Ex. 1001, 21:17–23, 22:15–22.

The parties disagree about whether each of limitations 1(d), 20(d), and 21(d) encompasses transmitting information to a protected network's IDS/IPS for the protection of endpoint devices in the network. Petitioner contends that it does. Pet. 33–34, 39–40; PO Resp. 18–43, 54; Reply 9–15; Sur-Reply 9–11. Patent Owner argues that “[t]he ’872 patent uses the term ‘computer system’ to refer to a computing device and not a network.” PO Resp. 24. Accordingly, Patent Owner contends that none of limitations 1(d), 20(d), and 21(d) encompasses mere transmission to an IDS/IPS of a protected network. *Id.* at 34–41.

We begin with the claim language in view of the Specification, which weighs heavily against Patent Owner's position that we should rewrite “computer system” as narrowly referring to a “computing device.” PO Resp. 24. As Petitioner notes, the ’872 patent's Specification uses “computer system” to refer to a wide range of equipment, from a component of a computing device, to a whole computing device, to a collection of computing devices. Reply 9–10 (citing Ex. 1001, 4:5–8, 11:15–18, 16:50–55). In one example, the Specification refers to “one or more other computer systems (e.g., protected network devices 136).” Ex. 1001, 18:52–53. Thus, the Specification lists “protected network devices 136” as only an example of “other computer systems,” demonstrating that “computer systems” refers to things other than protected network devices. Although Patent Owner may be correct that this passage

by itself does not convey “that ‘computer system’ encompasses anything more than a single computing device,” we find that other disclosures in the ’872 patent do.

Specifically, the Specification uses the language “distributed computer system” when referring to numerous components, including “protected network devices” and an “IDS/IPS system.” Ex. 1001, 3:26–28; Reply 10. In addition to showing that a “computer system” is not limited to a single computing device, this conveys that a “computer system” according to the ’872 patent can include an IDS/IPS.

Patent Owner argues that “a ‘distributed computer system’ is not necessarily a type of ‘computer system’ any more than a ‘stuffed animal’ is necessarily a type of animal, or ‘virtual reality’ is necessarily a type of reality.” PO Resp. 31. We find that argument unpersuasive. As Petitioner explains, the ’872 patent’s “distributed computer system” is a collection of actual computing devices, not an artificial or metaphorical concept. Reply 13.

Patent Owner also argues that the ’872 patent’s “‘distributed computer system 100’ is indisputably *not* an embodiment of the claimed ‘one or more computer systems other than the first computer system’ to be protected.” PO Resp. 31. Patent Owner further argues that the ’872 patent never refers to a network or an IDS as a “computer system.” *Id.* at 28–29, 35. At most, these observations minimally undermine Petitioner’s claim-construction position. As discussed above, the ’872 patent uses the term “computer system” in a manner that shows it refers to a wide range of equipment. Reply 9–10.

Patent Owner also argues that the claims show “computer system” cannot encompass a network. PO Resp. 25–26. Patent Owner notes that claim 1’s preamble “recites that ‘the first computer system [is] attached to a

computer network.” *Id.* at 25. Patent Owner argues that “[i]f a computer system were a network, the phrase ‘attached to a computer network’ would be superfluous and nonsensical.” *Id.* at 26. This argument is unpersuasive because it overlooks that one computer network could be attached to either a computer or another computer network, either or both of which could be referred to as a “computer system.” Patent Owner also contends that the “first computer system” cannot be a network because a computer system logically cannot connect to itself. *Id.* at 25–26. As discussed below in Section III.C.2.a).(5), this argument is inapposite because Petitioner’s mapping of Capalik’s components to the claims does not suggest a computer system (or any component) connected to itself.

Further weighing significantly in Petitioner’s favor, the parties agree that Patent Owner’s proposed construction would exclude some of the ’872 patent’s disclosed embodiments. PO Resp. 34–36; Reply 13–14; Ex. 1001, 18:44–58. Specifically, Patent Owner’s proposed construction would exclude embodiments in which “the decoy network device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.” Ex. 1001, 18:47–51. As Petitioner argues, we generally do not construe a claim as excluding disclosed embodiments. *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276–1277 (Fed. Cir. 2008).

Patent Owner argues that the facts here favor construing the claim to exclude a disclosed embodiment, citing *Baran v. Med. Device Techs.*, 616 F.3d 1309, 1314–16 (Fed. Cir. 2010). PO Resp. 35. We disagree. In *Baron*, the court explained that “[i]t is not necessary that *each* claim read on every embodiment.” 616 F.3d at 1316 (emphasis added). Noting that another claim read “on both the single-use and the reusable embodiments,” the court

construed claim 2 as reading on “only the reusable embodiment” (thereby excluding the single-use embodiment). *Id.* at 1316. The facts differ here. Claims 1, 20, and 21 are the ’872 patent’s only independent claims. If these claims were construed as excluding the ’872 patent’s disclosure of an embodiment transmitting information to a protected network’s IDS/IPS, then *no* claim would read on that embodiment. Moreover, in *Baron*, the court’s construction of “detachable” was based on the patent’s description of embodiments that were in “contrast” to one another. *Id.* at 1314–15. Here, the ’872 patent describes different embodiments, but they are not in “contrast.” *See*, Ex. 1001, 18:44–52. Additionally, *Baron* contains no indication that the patent there used the construed term (“detachable”) as broadly as the ’872 patent uses the term “computer system.” *See id.* at 1314–1316.

Patent Owner further argues that the prosecution history demonstrates that it “knew how to claim transmitting information to an IDS” but deliberately chose not to here. PO Resp. 37–38. For example, Patent Owner explains that it “explicitly claimed transmitting information to an IDS in the *Capalik* reference and other related patents that are incorporated by reference into the ’872 patent.” *Id.* at 38. Patent Owner emphasizes that “U.S. Patent 8,656,493 (Ex.2036) (“*Capalik* 493”), which is a continuation of the same parent application as *Capalik*, expressly recites both a “computer system” and an “intrusion prevention system” in the claims. *Id.* At most, this evidence tends to show that “computer system” is not coextensive with “intrusion prevention system” (or similar terms). It is not persuasive evidence that “computer system” does not encompass a protected network that includes an IDS/IPS.

Additionally, Patent Owner argues that the intrinsic and extrinsic evidence includes various other documents that reflect a meaning of “computer system” consistent with Patent Owner’s understanding. PO Resp. 39–41. We find these arguments unpersuasive in comparison to Petitioner’s strong arguments about the ’872 patent’s claims and Specification, such as Petitioner’s arguments that the Specification uses “computer system” broadly and discloses an embodiment that Patent Owner’s construction would exclude. Reply 15.

Patent Owner also argues that Petitioner’s construction makes the claim term “boundless,” “unintelligible,” and “indefinite.” PO Resp. 36–37. In support, Patent Owner argues that Petitioner’s expert “analogized his (and the Board’s) construction of ‘computer system’ to ‘**dough**’ that can be shaped and cut in ‘many, many ways’ to suit his needs.” *Id.* at 36 (citing Ex. 2033, 57:7–24. We find Patent Owner’s abstract question about the outermost limits of the term “computer system” inapposite to the actual claim-construction issue in this matter. In order to resolve the parties’ patentability dispute, we need only resolve whether “computer system” is limited to a “computing device” or is broad enough to encompass a protected network with an IDS/IPS and protected endpoint devices. *Realtime Data* 912 F.3d 1375.

Having considered all of the arguments and evidence, we conclude that the correct construction of “computer system” does encompass a protected network with an IDS/IPS and protected endpoint devices. Pet. 33–34, 39–40; PO Resp. 18–43, 54; Reply 9–15; Sur-Reply 9–11.

2. *Claim 2*

Claim 1 recites “monitoring activity on the first computer system.” Ex. 1001, 19:44. Claim 2 depends from claim 1 and requires that “the

monitoring further comprises monitoring all activity on the first computer system.” *Id.* at 19:60–62.

The parties disagree about the scope of claim 2. Petitioner suggests that claim 2 is taught by Capalik’s system “monitor[ing] all activity on the [virtual machine] that begins with a connection through a [virtual machine] network port.” *See* Pet. 34 (citing Ex. 1003 ¶¶ 145–146). Petitioner similarly contends that “monitor[ing] all *attack* activity in [a] *virtual machine* running on the decoy device . . . is what claim 2 is talking about.” Tr. 27:19–20 (emphasis added); Reply 16–17. In sum, Petitioner’s position is that claim 2’s “monitoring all activity on the first computer system” only requires monitoring attack activity that occurs on a virtual machine. Tr. 27:19–20 (emphasis added); Reply 16–17.

Patent Owner counters that claim 2 is an unqualified requirement for monitoring all activity on the first computer, not just monitoring “all attack activity on the virtual machine.” *See* Tr. 58:6–12. According to Patent Owner, “[m]onitoring that begins at a network-port/socket connection is not ‘monitoring all activity’ on the first computer: it omits local activity that occurs absent any socket event, including file process activities that the ’872 patent detects before any network access.” PO Resp. 44–45. Patent Owner also argues that claim 2’s “monitoring all activity on the first computer system” is not met by merely “monitoring all activity ‘on the [virtual machine] within the computer system.’” PO Resp. 51.

Thus, the parties raise two claim-construction issues: (1) whether the claim requires monitoring activity that is not attack activity, and (2) whether the claim requires monitoring activity happening in a computer system outside of the computer system’s virtual machine. Pet. 34; PO Resp. 43–54; Reply 16–20; Sur-Reply 11–15. Below, we address the first issue, which is

dispositive for the parties' patentability dispute. Accordingly, we do not reach the second issue.

Starting with the claim language itself, we agree with Patent Owner that monitoring attack activity is not the plain meaning of "monitoring all activity." Sur-Reply 13 (arguing we should reject Petitioner's attempt to rewrite claim's plain language); Tr. 58:6–10. We find this especially so in view of claim differentiation between claims 1 and 2. Claim 1's recitation of "monitoring activity on the first computer system" facially would encompass monitoring at least some activity, e.g., monitoring attack activity. Ex. 1001, 19:44. Because claim 2 expressly narrows from claim 1's scope of monitoring at least some activity to "monitoring all activity," we find that merely monitoring attack activity does not meet the plain meaning of claim 2. Indeed, Petitioner does not argue that its understanding of claim 2 reflects the plain meaning of the claim language. *See generally* Pet.; Reply; Tr.

Next, we consider whether other evidence warrants deviating from the claim's plain meaning. Petitioner contends that the '872 patent teaches leaving its virtual machine intentionally open to attacks and "exclusively teach[es] monitoring attack activity in a [virtual machine], which has activity to monitor **only** when attacked." Reply 16 (citing Ex. 1001, 5:3–6). Citing Dr. Jakobsson's testimony, Petitioner contends that "**there is nothing to detect** unless the [virtual machine] is being attacked." *Id.* at 17 (citing Ex. 1035 ¶¶ 4–10).

The evidence fails to support key aspects of Petitioner's position. Dr. Jakobsson testifies that the '872 patent discloses monitoring attack activity. *E.g.*, Ex. 1035 ¶¶ 4, 8. But, contrary to Petitioner's suggestion, Dr. Jakobsson does not testify that the '872 patent teaches an absence of

non-attack activity on the virtual machine. *See, e.g., id.* ¶¶ 4–10. Rather, Dr. Jakobsson testifies that “[i]n . . . the ‘872 Patent . . . , the decoy device exists to be attacked, and until it has been attacked, there is no *attack* activity to monitor.” *Id.* ¶ 4 (emphasis added). This reflects the fact that the system can only monitor attack activity if there is an attack; it does not show that the virtual machine lacks non-attack activity, much less that the system does not monitor such non-attack activity.

Dr. Jakobsson also testifies that in the ‘872 patent “monitoring occurs in response to attack activity within the [virtual machine],” consistent with “a well-understood design in the filed in which instrumentation is triggered by attacker interaction with the decoy environment.” *Id.* ¶ 8. Although this testimony tends to show that the monitoring disclosed by the ‘872 patent includes monitoring attack activity, it does not persuasively support Petitioner’s position that the disclosed monitoring excludes other activity. *See* Reply 16. Nor do Petitioner’s and Dr. Jakobsson’s assertions that the ‘872 patent’s virtual machine exists to be attacked. *E.g.,* Reply 16–17; Ex. 1035 ¶¶ 4–5, 8.

Petitioner argues that the ‘872 patent’s disclosure starting at column 10, line 8 of the Specification teaches that “everything that is being monitored is attack activity.” Tr. 74:7–21. But this portion of the Specification discloses without qualification that “[i]n some embodiments, the introspection module monitors *all activity*.” Ex. 1001, 10:8–9 (emphasis added). As examples of the monitored activity, the ‘872 patent lists “system calls, library calls, kernal calls, etc.” *Id.* at 10:8–10. Petitioner does not provide a persuasive basis for its view that such activities are limited to attack activities. And certain portions of the Specification indicate that the system monitors more than attack activity. For example, the Specification

discloses that monitored activities may be “malignant, benign, etc.”
Ex. 1001, 12:30–34.

On the whole, we find the evidence does not warrant deviating from claim 2’s plain meaning, which is “monitoring *all* activity,” not just monitoring all attack activity. Ex. 1001, 19:61 (emphasis added).

3. *Claim 8*

Claim 7 recites “graphically displaying at least a subset of the stored activities.” Ex. 1001, 20:10–11. Claim 8 depends from claim 7 and recites “wherein the displaying includes visually distinguishing at least a subset of the associations.” *Id.* at 20:12–13. Petitioner takes the position that displaying only malignant associations meets claim 8’s “visually distinguishing at least a subset of the associations.” *See, e.g.*, Pet. 55 (“[A person of ordinary skill in the art] would have understood that *King’s* dependency graphs visually distinguish a subset of the associations by depicting only malignant associations in a filtered dependency graph.”); Reply 22 (“By displaying *only* malignant associations in its filtered graph, King is visually distinguishing the subset of associations that are malignant.”). Petitioner suggests that displayed malignant associations are distinguished from associations that are not displayed. Pet. 55; Reply 22–23. Patent Owner argues that “[m]erely displaying a subset does not ‘visually distinguish’ the subset.” PO Resp. 60.

Petitioner does not provide persuasive reasoning or evidence in support of its construction of claim 8. Petitioner does not argue or show that displaying only malignant associations is consistent with the plain meaning of “visually distinguishing at least a subset of the associations.” *See* Pet. 54–56; Reply 22–23.

Nor does Petitioner argue persuasively that the Specification suggests merely displaying malignant associations constitutes “visually distinguishing” as required by claim 8. Pet. 54–56; Reply 22–23. Rather, Petitioner argues that “[t]he ’872 Patent explains that, for example, a bold arrow can represent a malignant association and a regular arrow can represent a benign association.” Pet. 55 (citing Ex. 1001, 12:32–41). This example of visually distinguishing by displaying associations in *different ways* does not suggest that merely displaying malignant associations is visually distinguishing them.

Dr. Jakobsson passingly mentions the ’872 patent’s disclosure of visually distinguishing associations. Ex. 1003 ¶210. In addition to noting the example of bold and regular arrows, Dr. Jakobsson testifies that “[t]he ’872 patent explains . . . that any graphical scheme can be used to visually distinguish the subset of associations.” *Id.* But Dr. Jakobsson does not address the fact that the ’872 patent provides examples, none of which is displaying a malignant association: “any other graphical scheme can be used to visually distinguish the subset of associations, *such as color font, shape, icons, etc.*” Ex. 1001, 12:38–41 (emphasis added); Ex. 1003 ¶ 210. Although displaying malignant associations may be a graphical scheme, Dr. Jakobsson does not provide persuasive arguments or evidence that it constitutes “visually distinguishing at least a subset of the associations” in view of the ’872 patent’s disclosure. Ex. 1003 ¶¶ 188–212; Pet. 54–56; Reply 22–23.

In sum, on this record, the evidence does not support Petitioner’s position that displaying only malignant associations qualifies as “visually distinguishing at least a subset of the associations,” as recited in claim 8. This is dispositive for the parties’ claim 8 dispute. *See infra*

Section III.E.2.b). Accordingly, we need not further construe claim 8.
Realtime Data, LLC v. Iancu, 912 F.3d 1368, 1375.

C. GROUND 1 – ALLEGED OBVIOUSNESS OVER CAPALIK

1. Overview of Capalik

Capalik “relates to the field of methods and systems for protecting computer networks.” Ex. 1004 ¶ 2. Capalik discusses an embodiment in connection with Figure 5, which is reproduced below.

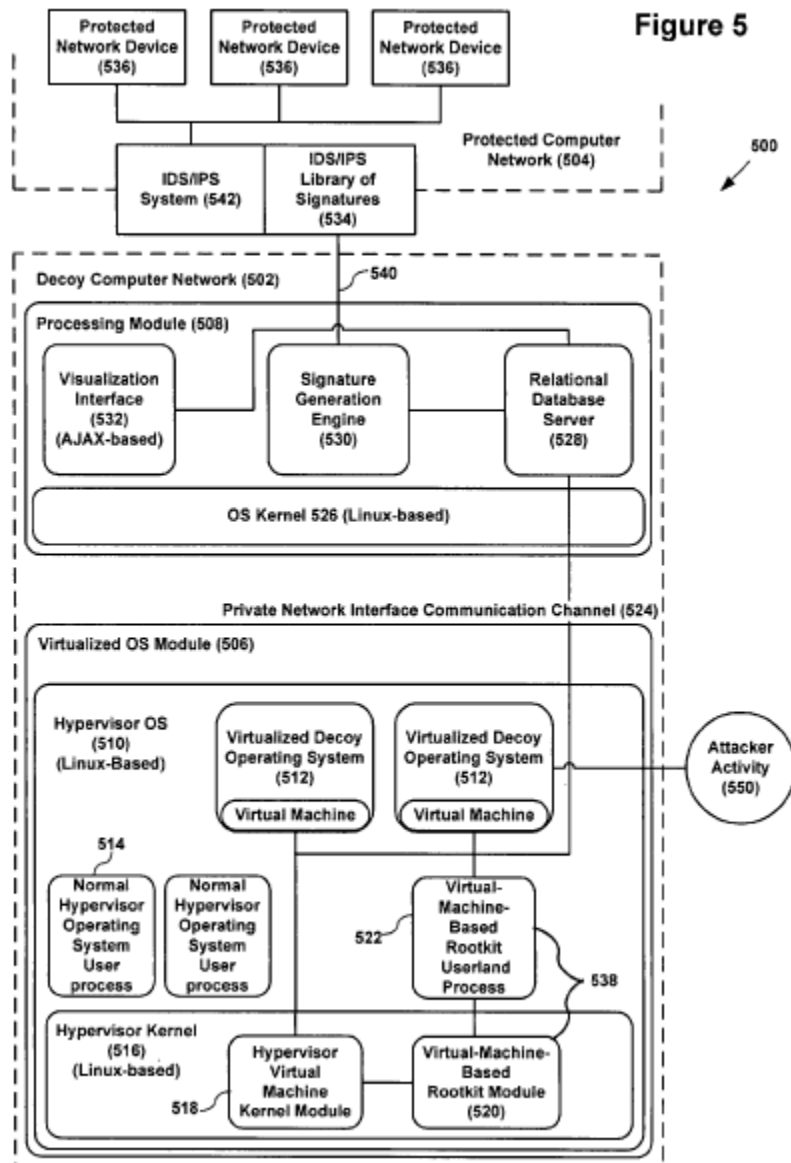


Figure 5 is a block diagram showing “a system for analyzing and preventing unauthorized intrusion into a computer network.” Ex. 1004 ¶¶ 20, 37.

Specifically, Figure 5 shows system 500, which comprises decoy computer network 502 and protected computer network 504. Ex. 1004 ¶ 38. “The decoy computer network 502 includes a virtualized operating system module 506 for monitoring the decoy network 502, and a processing module 508 for obtaining, analyzing, and responding to exploits.” *Id.* “The protected computer network 504 includes an IDS/IPS library of signatures 534 and an IDS/IPS system 542 coupled to multiple protected network devices 536.” *Id.* ¶ 53.

“In use, attacker activity 550 is directed at the decoy computer network 502 through one more ports . . . that are left open as a gateway for attacker activity.” Ex. 1004 ¶ 44. When an attacker connects to an open port, decoy computer network 502 “monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts.” *Id.* ¶ 49. Decoy computer system 502 stores attack information as forensic data. *Id.* ¶ 52. If an interaction warrants creating an attack signature, decoy computer network 502’s processing module 508 may generate an attack signature using the forensic data. *Id.* ¶¶ 52, 59. The attack signature may be sent “to the intrusion detection system (IDS) or intrusion prevention system (IPS) for the protected network 504.” *Id.* ¶ 59.

2. Discussion

In asserting obviousness of claims 1–6, 12, 15, 20, and 21 over Capalik, Petitioner argues that Capalik teaches all of the challenged claims’ limitations. Pet. 13–40. Patent Owner argues that Petitioner fails to show

that Capalik teaches claim 1's limitations 1(c) and 1(d), as well as claim 2. PO Resp. 14–54.

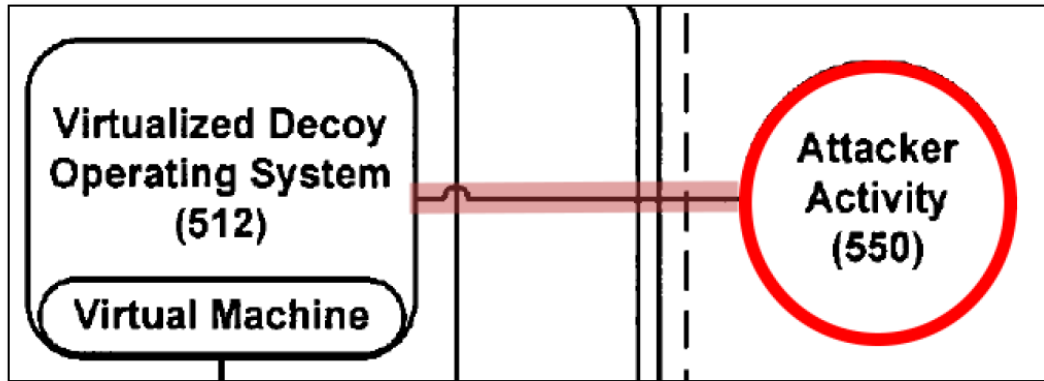
Having reviewed all of the parties' arguments and evidence, we determine Petitioner has shown unpatentability of the '872 patent's claims 1, 3–6, 12, 15, 20, and 21 over Capalik. Pet. 13–40; PO Resp. 14–43, 68–76; Reply 1–20, 26–29; Sur-Reply 1–15, 22–23. We determine that Petitioner has not shown unpatentability of claim 2 over Capalik. Pet. 34, PO Resp. 43–54; Reply 16–20; Sur-Reply 11–15. We turn now to detailed discussions of the claim challenges.

a) Claim 1

(1) Preamble

Claim 1's preamble recites “[a] computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory.” Ex. 1001, 19:39–43.

Petitioner contends that “[t]o the extent the Preamble is limiting, *Capalik* teaches it.” Pet. 13. Petitioner elaborates that “*Capalik* describes ‘a system for analyzing and preventing unauthorized intrusion into a computer network’ as shown in FIG. 5.” *Id.* (citing Ex. 1004 ¶ 37). Petitioner argues that an ordinarily skilled artisan “would have understood [Capalik’s] Decoy Computer System 502 is a first computer system” and includes one or more processors and memory. *Id.* at 15–16 (citing Ex. 1003 ¶¶ 106–107, 109–110; Ex. 1004 ¶ 39). Regarding the preamble’s recitation that the “first computer” is “attached to a computer network,” Petitioner and Dr. Jakobsson point to decoy computer system 512’s attachment to attacker activity 550, as shown by Dr. Jakobsson in the following annotated excerpt of Capalik’s Figure 5. Pet. 15; Ex. 1003 ¶ 107 (citing Ex. 1004 ¶ 44, Fig. 5).



Dr. Jakobsson’s annotated excerpt of Capalik’s Figure 5 includes a circular, red annotation on attacker activity 550, along with a linear, red annotation on the connection from attacker activity 550 to virtualized decoy operating system (512). Ex. 1004 ¶ 7.

Patent Owner does not dispute Petitioner’s arguments and evidence for claim 1’s preamble. *See generally* PO Resp. We find Petitioner shows by a preponderance of the evidence that Capalik teaches claim 1’s preamble. Pet. 13.

(2) *Limitation 1(a)*

Limitation 1(a) recites “monitoring activity on the first computer system.” Ex. 1001, 19:44.

Petitioner contends that Capalik teaches this limitation. Pet. 16–22. Petitioner argues that Capalik discloses monitoring computer system activity “using a VM [(virtual machine)] and VMM [(virtual machine monitor)] system”:

Like the ’872 Patent, *Capalik* describes Hypervisor OS 510 (annotated green), “also known as a virtual machine monitor operating system[.]” *Capalik*, [0040]. Within Hypervisor OS 510, multiple Virtual Machines . . . exist in the form of “virtualized operating systems 512 [and] act as decoy operating systems to attract attacker activity 550.” *Id.*

Hypervisor kernel 516 (annotated orange) “is that part of the hypervisor operating system 510 that resides in physical memory at all times and provides the basic services to the hypervisor operating system 510.” *Id.* [0041]. “[T]he virtual machine-based rootkit module 520 and its associated userland processes 522 constitute an **introspection module 538** [(annotated blue)] (also known as a virtual machine-based memory introspection analysis tool) that **monitors and introspects into the virtualized decoy operating systems memory segments.**” *Id.*, [0047].

Id. at 21.

Patent Owner does not dispute Petitioner’s arguments and evidence for limitation 1(a). *See generally* PO Resp. We find Petitioner shows by a preponderance of the evidence that Capalik teaches limitation 1(a). Pet. 16–22.

(3) Limitation 1(b)

Limitation 1(a) recites “identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target.” Ex. 1001, 19:45–49.

Petitioner contends that Capalik teaches this limitation. Pet. 22–26. Petitioner argues that it would have been understood by an ordinarily skilled artisan “that *Capalik* teaches identifying a plurality of activities wherein each activity includes an activity source (e.g., data packet stream), an activity target (e.g., socket receiving the data packet stream), and an association between the activity source and activity target (e.g., receiving the data packet stream at the socket).” *Id.* at 22. Petitioner cites Capalik’s process of monitoring, storing, and reporting attacker activity:

Capalik discloses that when an attacker connects to a network port and begins interacting with virtualized decoy operating system 512 (within the virtualized operating system module 506)

Capalik's introspection module 538, "monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts." *Capalik* [0049]. The captured information is then (1) sent to processing module 508, (2) stored in relational database server 528, and (3) used to generate an attack report. *Capalik*, [0050], [0052], [0055].

Id. at 23. After explaining the nature of *Capalik*'s report and the sources, targets, and associations (*id.* at 23–26), Petitioner concludes that "[b]ecause *Capalik* monitors and reports the full 'path' or series of actions between a plurality of activity sources and activity targets, a POSITA would have understood that *Capalik* teaches identifying associations between each set of the plurality of activity sources and activity targets" (*id.* at 27 (citing Ex. 1003 ¶¶ 128–129)).

Patent Owner does not dispute Petitioner's arguments and evidence for limitation 1(b). *See generally* PO Resp. We find Petitioner shows by a preponderance of the evidence that *Capalik* teaches limitation 1(b). Pet. 22–26.

(4) *Limitation 1(c)*

Limitation 1(c) recites "storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities." Ex. 1001, 19:50–52.

Petitioner argues that *Capalik* teaches this limitation. Pet. 27–30; Reply 4–9. Referring to arguments and evidence addressing limitation 1(b), Petitioner argues that "*Capalik* teaches identifying activity sources, activity targets, and associations." Pet. 27. Petitioner elaborates that *Capalik* teaches monitoring, storing, and analyzing "attack information":

Capalik teaches virtualized operating system module 506 monitors decoy network 502, and processing module 508 obtains, analyzes, and responds to malicious exploits. *Capalik*, [0038]. Processing module 508 comprises Relational Database Server 528 (annotated blue), which stores “attack information” as forensic data for later analysis. *Capalik*, [0052]; *see also, id.* [0048] (“the introspection module 538 examines the contents of the decoy operating systems’ 512 memory segments in **an instrumented context that generates and retrieves forensic data** for analysis by the processing module 508.”).

Id. at 28–29. Petitioner argues that an ordinarily skilled artisan would have understood “*Capalik*’s ‘forensic data’ is stored in a data structure, as claimed, at least because the stored data is used by ‘[t]he signature generation engine 530 . . . to generate a signature of the attack.’” *Id.* at 29 (citing Ex. 1004 ¶ 52; Ex. 1001, 10:33–36; Ex. 1003 ¶¶ 134–136). More specifically, Petitioner argues that an ordinarily skilled artisan would have understood *Capalik* stores activity sources, targets and associations in a data structure:

As explained above at Claim [1(b)], *Capalik*’s attack report includes activity sources and targets, and the corresponding associations. Accordingly, a POSITA would have understood that the “attack information” or “attack-identifying information” stored in relational database server 528 as a forensic data structure, and used to create the attack report, includes activity sources, targets, and associations.

Id. at 30.

Patent Owner counters that Petitioner fails to show that *Capalik* teaches or suggests the claimed data structure. PO Resp. 14–18; Sur-Reply 1–9. Patent Owner contends that Petitioner “points to zero explicit disclosure in *Capalik* of a data structure, let alone one that identifies for each of a plurality of activities, the sources, targets, and associations between the sources and targets.” PO Resp. 15–16. Patent Owner further

argues that Petitioner’s evidence does not show that an ordinarily skilled artisan would have understood Capalik teaches such a data structure.

Id. at 15–18. Patent Owner characterizes Dr. Jakobsson’s testimony as conclusory, faulting his logic as insufficiently supporting his conclusions. *Id.* at 14, 16–17. Patent Owner also argues that the ’872 patent’s figures show data structures not shown or discussed in Capalik. *Id.* at 18.

Reviewing the parties’ arguments and evidence, we find that Petitioner demonstrates by a preponderance of the evidence that an ordinarily skilled artisan would have understood that Capalik teaches limitation 1(c). Pet. 22–30; PO Resp. 14–18; Reply 4–9; Sur-Reply 1–9. As discussed above in Sections III.C.2.a).(2), (3), we find persuasive Petitioner’s undisputed arguments and evidence that Capalik monitors, captures, stores, and reports information identifying sources, targets, and associations of activities. Pet. 22–27. Those undisputed arguments and evidence establish that Capalik teaches most of limitation 1(c), leaving only the question of whether Capalik stores the information in a “data structure.”

In response to Petitioner’s argument that Capalik stores the information in a data structure, Patent Owner contends that Capalik stores the forensic data as unstructured data. *E.g.*, Tr. 7:19–25, 10:17–11:15, 42:18–43:3, 47:2–7. We find Petitioner’s position better supported. Capalik describes capturing and storing attack information as forensic data for signature generation nearly identically to the ’872 patent’s disclosure of capturing and storing attack information as forensic data for signature generation. *Compare* Ex. 1004 ¶¶ 52 with Ex. 1001, 10:30–36; *see also* Reply 2–3 (comparing disclosures). In particular, Capalik discloses storing the information in relational database server 528. Ex. 1004 ¶ 52; Pet. 27–29.

Patent Owner does not dispute Petitioner's position that a relational database like Capalik's is a data structure. Tr. 10:12–23, 41:10–16.

In view of this and Capalik's disclosure of using the stored information to generate an attack signature or report, Dr. Jakobsson credibly testifies that Capalik's captured information identifies activity sources, activity targets, and associations, and that an ordinarily skilled artisan would have understood that Capalik stores this information in a data structure. Ex. 1003 ¶¶ 130–136. Contrary to Patent Owner's argument that the testimony is conclusory, we find Dr. Jakobsson's detailed reasoning logically sound and well-supported by his citations to Capalik, the '872 patent, and other evidence showing the known practice of storing data in data structures. Ex. 1003 ¶¶ 130–136 (citing Ex. 1004 ¶¶ 38, 39, 48, 52, 55, 56; Ex. 1001, 6:10–17, 10:33–36, Fig. 2; Ex. 1015, 3:51–4:60, Fig. 2; Ex. 1008, Figs. 5B–5C). Collectively, Petitioner's arguments and evidence soundly support Petitioner's position that an ordinarily skilled artisan would have understood that Capalik stores information identifying the activities' sources, targets, and associations in a data structure. Pet. 22–30; Ex. 1003 ¶¶ 118–136; Reply 1–9.

And on the whole, the evidence weighs against Patent Owner's position that Capalik stores its forensic attack information as unstructured data. Tr. 47:6–7 (“[Capalik's data] is unstructured, Your Honor. It is just forensic data.”). Patent Owner argues that Capalik does not expressly refer to a “data structure.” PO Resp. 16. Patent Owner further argues that an ordinarily skilled artisan “would not have inferred a ‘data structure that identifies the activity sources, the activity targets, and the associations’ from the mere fact that Capalik's forensic data is used to generate a report or signature.” *Id.* at 17 (citing Ex. 2031 ¶ 59). Patent Owner reaches this

conclusion because “[r]eports and signatures can be generated from unstructured data using intermediate processing; neither the reports nor the act of generating such reports retroactively supply the missing data structure.” *Id.*

These arguments do not persuasively rebut Petitioner’s position. Petitioner’s observation that Capalik generates a signature or report from its forensic data ties together with other evidence, such as Capalik’s disclosure of storing the information in a relational database, to show that an ordinarily skilled artisan would have understood that Capalik stores its forensic data in a data structure. Pet. 22–30; Ex. 1003 ¶¶ 118–136; Reply 1–9. This outweighs Patent Owner’s arguments that Capalik’s omission of the words “data structure” comes with a possibility of generating a report from unstructured data. Reply 17; *In re Preda*, 401 F.2d 825, 826 (CCPA 1968) (“[I]n considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom.” (citing *In re Shepard*, 319 F.2d 194, 50 CCPA 1439 (1963))).

We also find little persuasive weight in Patent Owner’s argument that the ’872 patent distinguishes over Capalik because the ’872 patent discusses certain data structures shown in its Figures 3A–3C, 4A–4E, and 5A–5C, which do not appear in Capalik. Reply 18; Sur-Reply 3–6. The parties agree that the claimed “data structure” is not limited to any particular data structure, much less the specific examples in the ’872 patent’s figures. Pet. 29; Tr. 50:17–25. Thus, Capalik need not disclose those specific data structures to teach limitation 1(c). To the extent Patent Owner suggests that Capalik fails to teach a data structure because it does not expressly discuss

which organization scheme is used in its relational database, we disagree. *See Preda*, 401 F.2d at 826.

Patent Owner also argues that Petitioner’s “own analysis under [limitation 1(d)] underscores the gap.” PO Resp. 17. Patent Owner explains that, when addressing limitation 1(d), Petitioner did not allege that Capalik’s signature identifies sources or associations. *Id.* at 17–18. This argument unpersuasively attempts to sidestep Petitioner’s undisputed arguments and evidence for limitations 1(b) that Capalik captures and processes information identifying sources, targets, and associations. Pet. 22–27; Reply 5.

In sum, Petitioner shows by a preponderance of the evidence that an ordinarily skilled artisan would have understood Capalik teaches limitation 1(c).

(5) *Limitation 1(d)*

As noted above, limitation 1(d) recites the following:

transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:53–59.

Addressing this limitation, Petitioner cites Capalik’s disclosure of transmitting an attack signature generated at decoy computer network 502 to protected computer network 504. Pet. 33 (citing Ex. 1004 ¶¶ 52, 53, 59, Fig. 5; Ex. 1003 ¶¶ 143–144). Petitioner argues that Capalik “teaches that once the attack signature is generated, it can be sent ‘to the intrusion detection system (IDS) or intrusion prevention system IPS) for the protected network 504.’” *Id.* (citing Ex. 1004 ¶¶ 53, 59; Ex. 1003 ¶¶ 143–144).

Petitioner contends that “a [person of ordinary skill in the art] would have understood that *Capalik* transmits the fingerprint, including information identifying one or more of the activity sources, the activity targets, and the associations to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.” *Id.* at 34 (citing Ex. 1003 ¶¶ 137–144). Petitioner elaborates that “[a person of ordinary skill in the art] would have further understood that *Capalik* transmits this information to a computer system other than computer decoy 502 since the signature is sent ‘through a standard network connection’ to IDS/IPS 534 of protected network 504.” *Id.* (citing Ex. 1004 ¶ 59, Fig. 5; Ex. 1003 ¶¶ 137–144).

Patent Owner counters that *Capalik* does not disclose limitation 1(d). PO Resp. 18–43. Specifically, asserting that claim 1’s “‘computer system’ is a computing device, not multiple computing devices and not a computer network,” Patent Owner argues that “[u]nder this correct construction, [Petitioner] has no argument and all the grounds fail against each claim.” *Id.* at 43. Based on this claim-construction position, Patent Owner argues that *Capalik* does not disclose transmitting its signature to any single protected device. PO Resp. 20–23. This argument is unavailing because, as discussed above in Section III.B.1, the evidence supports Petitioner position that limitation 1(d)’s “computer system” encompasses a protected network with an IDS/IPS and protected endpoint devices.

Patent Owner further suggests that *Capalik*’s protected computer network 504 logically cannot correspond to a “computer system.” PO Resp. 25–26. Patent Owner argues that “[t]he preamble of claim 1 recites that the first computer system [is] attached to a computer network.” *Id.* at 25. Patent Owner then asserts that “[i]f a computer system were a network, the phrase ‘attached to a computer network’ would be superfluous and

nonsensical.” *Id.* at 26. Contrary to Patent Owner’s suggestion, Petitioner’s arguments do not indicate that any Capalik component attaches to itself. When addressing the claim language “a first computer system attached to a computer network,” Petitioner argues that “*Capalik’s* Decoy Computer 502 is attached to a computer network. Namely, *Capalik* teaches ‘attacker activity 550 is directed at the [D]ecoy [C]omputer[] 502 through one more ports of each of the virtualized decoy operating systems 512 that are left open as a gateway for attacker activity 550.’” Pet. 15. Thus, Petitioner argues that decoy computer 502 corresponds to claim 1’s “first computer system” and attaches to a network identified at 550, which does not suggest that any Capalik component attaches to itself. Petitioner’s logically consistent mapping of claim 1’s limitations to Capalik’s disclosure prevail over Patent Owner’s abstract argument that a component cannot connect to itself. *E.g.*, Pet. 13–16, 30–34; PO Resp. 25–26; Reply 11.

Reviewing the parties’ arguments and evidence, we determine that Petitioner has shown by a preponderance of the evidence that Capalik teaches limitation 1(d). Pet. 30–34; PO Resp. 18–43; Reply 9–15; Sur-Reply 9–11.

(6) *Objective Indicia*

Patent Owner contends that objective indicia of non-obviousness weigh against obviousness of the claims. PO Resp. 68–76. Patent Owner argues that Petitioner developed its commercial product by copying Patent Owner’s earlier patent applications and thereby achieved commercial success and industry praise. *Id.* Petitioner counters that Patent Owner “has insufficient evidence of secondary considerations to overcome the strong case of obviousness.” Reply 26.

We agree with Petitioner. Specifically, having considered the parties' arguments and evidence, we determine that Patent Owner fails to sufficiently show a nexus between any of its objective indicia evidence and the claimed invention. *See Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) ("The patentee bears the burden of showing that a nexus exists"). A showing of sufficient nexus is required to establish that the evidence relied upon traces its basis to a novel element in the claim, not to something in the prior art. *Institut Pasteur & Universite Pierre Et Marie Curie v. Focarino*, 738 F.3d 1337, 1347 (Fed. Cir. 2013). Objective evidence that results from something that is not "both claimed and novel in the claim" lacks a nexus to the merits of the invention. *In re Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (emphasis omitted). Thus, establishing nexus involves a showing that novel elements in the claim, not prior-art elements, account for the objective evidence of nonobviousness. *Id.*

As discussed above, Petitioner shows that Capalik teaches all limitations of claim 1. Petitioner persuades us that none of claim 1's elements individually nor any combination thereof is novel over Capalik's disclosure. Accordingly, claim 1 is not novel over Capalik, which disproves Patent Owner's assertion of nexus. PO Resp. 73–76.

Moreover, even if claim 1 were novel, Patent Owner otherwise fails to show nexus for its commercial success, praise, or copying assertions. Patent Owner's evidence does not show that Petitioner's commercial product embodies claim 1. For example, we agree with Petitioner that Patent Owner "failed to analyze any meaningful detail regarding" how the Falcon Platform allegedly meets limitation 1(d). Reply 28–29. In particular, Patent Owner has not sufficiently addressed limitation 1(d) with the following argument: "**1[D]** The Falcon Platform transmitted to other computer systems

information identifying the sources, targets, and associations for preventing future attacks against those computer systems: The Falcon Platform “[s]hares information across an entire community of like like-minded trusted defenders.” PO Resp. 72 (citing Ex. 2015, 1; Ex. 2031 ¶ 103).

Additionally, Petitioner provides another, independent reason that Patent Owner’s copying assertions fail. Addressing Patent Owner’s suggestion that Mr. Alperovitch was exposed to and copied the ’872 patent’s parent application, Petitioner cites evidence that Mr. Alperovitch also was exposed to Capalik. Reply 27. Given this, Petitioner explains that Patent Owner “would have to—but cannot—demonstrate that Mr. Alperovitch took with him and implemented in CrowdStrike’s system the ’872 Patent’s teachings *in isolation from* Capalik’s.” *Id.* Patent Owner neither disputes that Mr. Alperovitch was exposed to Capalik nor otherwise persuasively rebuts Petitioner’s argument. *See* Sur-Reply 22–23.

(7) *Claim 1 Conclusion*

Having reviewed all of the parties’ arguments and evidence, we find Petitioner has shown unpatentability of claim 1 over Capalik by a preponderance of the evidence. Pet. 13–34; PO Resp. 1–43; Reply 1–15; Sur-Reply 1–11.

b) *Claim 2*

Claim 2 recites “the method of claim 1, wherein the monitoring further comprises monitoring all activity on the first computer system.” Ex. 1001, 19:44, 19:60–62. According to Petitioner, “a [person of ordinary skill in the art] would have understood that *Capalik* teaches monitoring all activity on the computer system.” Pet. 34 (citing Ex. 1004 ¶¶ 49, 59; Ex. 1003 ¶¶ 145–146). In the Petition, Petitioner asserted that Capalik “teaches monitoring all activity on the [virtual machine].” *Id.*

Patent Owner counters that Petitioner fails to show that Capalik teaches monitoring all activity on its virtual machine. PO Resp. 44 (citing Pet. 34). According to Patent Owner, Petitioner cites evidence of monitoring activity that begins at a socket, but does not account for activity that happens without a socket event. *Id.* at 44–45.

Subsequently, Petitioner clarified that its position is Capalik meets claim 2 because “Capalik monitors all *attack* activity in its virtual machine running on the decoy device.” Tr. 27:19–20 (emphasis added); *see id.* at 33:8–35:14; Reply 16 (“Capalik Monitors All Attack Activity, Satisfying Claim 2”). As explained above in Section III.B.2, the evidence does not support Petitioner’s contention that claim 2 only requires monitoring all *attack* activity. Accordingly, even if Capalik does teach monitoring all attack activity, that alone does not meet Petitioner’s burden.

Petitioner further suggests that, in the particular system disclosed by Capalik, monitoring all attack activity on the virtual machine is monitoring all activity on the virtual machine. *See* Reply 16–17; Tr. 31:1–33:14. In support of this, Petitioner argues that the only activity on Capalik’s virtual machine is attack activity. Reply 16 (“Capalik . . . exclusively teach[es] monitoring attack activity in a [virtual machine], which has activity to monitor *only* when attacked.”); Tr. 31:1–33:14.

But the evidence does not show that the only activity that happens on Capalik’s virtual machine is attack activity. Reply 16–17 (citing Ex. 1045 ¶ 45; Ex. 1035 ¶¶ 4–10); Tr. 31:1–33:14 (citing Ex. 1003 ¶¶ 145–146; Ex. 1004 ¶¶ 49, 59). Capalik discloses decoy operating system 512 interacting with an attacker, followed by possible generation of an attack signature. *E.g.*, Ex. 1004 ¶¶ 45, 49, 59. This does not show that attack

activity is the only activity on Capalik's virtual machine because it does not preclude other activity as well.

Nor does Petitioner's other evidence. For example, the Petition contends that Dr. Jakobsson's first declaration "explain[s] that a [person of ordinary skill in the art] would have understood *Capalik's* detailed forensic data monitors all activity on the [virtual machine] that begins with a connection through a [virtual machine] port." Pet. 34 (citing Ex. 1003 ¶¶ 145–146). Assuming that Petitioner is correct that Capalik monitors all activity that starts at a virtual machine port, that does not show that Capalik's virtual machine lacks any other activity, i.e., activity that does not start at a port.

Dr. Jakobsson's reply testimony also falls short of supporting Petitioner's position. Ex. 1035 ¶¶ 4–10. Contrary to Petitioner's suggestion, Dr. Jakobsson's reply testimony does not show that the only activity on Capalik's virtual machine is attack activity. *Id.* For example, Dr. Jakobsson testifies that Capalik's "decoy device exists to be attacked, and until it has been attacked, there is no *attack* activity to monitor." *Id.* ¶ 4 (emphasis added). Dr. Jakobsson similarly testifies that there is no attack activity to monitor on Capalik's virtual machine before an attack happens:

[u]ntil [attack activity within the virtual machine] occurs, there is no *attack* behavior to monitor, identify, record, or analyze. Accordingly, the decoy system is designed to monitor and identify activity once an attacker engages with the [virtual machine]. *It is not*, as [Patent Owner] and Dr. Stavrou suggest, *designed to monitor or identify non-attack activity* in isolation from a detected attacker access.

Id. ¶ 8 (emphases added). Contrary to Petitioner's position that only attack activity happens on Capalik's virtual machine, this testimony suggests that

Capalik’s virtual machine activity includes “non-attack activity” that is not all monitored.

Dr. Jakobsson’s cross-examination testimony comports with this. Ex. 2053, 125:5–127:18. After acknowledging Capalik’s disclosure that its “front end presents a standard fully functional operating system such as Windows or a flavor of Linux or Sun Microsystems Solaris” (*id.* at 125:5–13), Dr. Jakobsson testified that the operating system performs tasks without user intervention (*id.* at 127:4–18). *See also* Sur-Reply 14 (citing Dr. Jakobsson testimony, arguing “Capalik uses conventional operating system to provide illusion of a vulnerable computer”). Dr. Stavrou similarly testifies that “Capalik does not disclose or suggest monitoring internal system-level activity, such as changes to local files, unauthorized process behavior, or movement across virtual machines or system components.” Ex. 2031 ¶ 68.

Dr. Jakobsson also testifies that “[h]oneypots and other decoy systems were well known” ways to lure attacks and gather attack information useful for protecting against intrusions. Ex. 1003 ¶¶ 49–54. Dr. Jakobsson adds that “[h]oneypots and decoy systems were known to both monitor all activity at the decoy system as well as assume all activity was unauthorized.” *Id.* ¶ 146 (citing *id.* ¶¶ 49–54). We note that, in his first declaration, Dr. Jakobsson states without qualification that “a [person of ordinary skill in the art] would have understood that *Capalik* teaches monitoring all activity on the computer system.” Ex. 1003 ¶ 146. But Dr. Jakobsson supports this with general assertions in the vein of “[h]oneypots and decoy systems were known to both monitor all activity at the decoy system as well as assume all activity was unauthorized.” *Id.* We agree with Patent Owner that this testimony is not persuasive to show that an ordinarily skilled artisan would

have understood that Capalik monitors all virtual-machine activity, including internal activity not initiated at a port. PO Resp. 49–51.

In sum, weighing the parties’ arguments and evidence, Petitioner’s contention that an ordinarily skilled artisan “would have understood that *Capalik* teaches monitoring all activity on the computer system” is not shown by a preponderance of the evidence. Pet. 34; PO Resp. 43–54; Reply 16–20; Sur-Reply 11–15. Having reviewed all of the parties’ arguments and evidence, we find Petitioner has not shown unpatentability of claim 2 by a preponderance of the evidence. Pet. 34; PO Resp. 43–54; Reply 16–20; Sur-Reply 11–15.

3. *Claims 3–6, 12, 15, 20, and 21*

Petitioner argues that Capalik teaches all limitations of claims 3–6, 12, 15, 20, and 21. Pet. 35–40. Patent Owner counters that the alleged deficiencies in in Petitioner’s claim 1 challenge render deficient the challenge to claim 3–6, 12, 15, 20, and 21. PO Resp. 54. As explained above in Section III.C.2.a), we do not find any deficiency in Petitioner’s claim 1 challenge. Having reviewed all of the parties’ arguments and evidence, we find Petitioner shows by a preponderance of the evidence that Capalik teaches all limitations of claims 3–6, 12, 15, 20, and 21. Pet. 35–40; PO Resp. 54.

Regarding objective indicia of nonobviousness, Patent Owner has not shown a nexus to any of claims 3–6, 12, 15, 20, and 21. Petitioner has shown that Capalik teaches all limitations of claims 3–6, 12, 15, 20, and 21. Petitioner persuades us that none of these claims’ elements is novel individually, and that none of the claims recites a combination of elements that is novel over Capalik. Pet. 35–40. Accordingly, claims 3–6, 12, 15, 20, and 21 are not novel over Capalik, and Patent Owner therefore does not

establish nexus. *Kao*, 639 F.3d at 1068 (Objective evidence that results from something that is not “both claimed and novel in the claim” lacks a nexus to the merits of the invention). Additionally, beyond the shortcomings for claim 1 discussed above, Patent Owner does not even assert that Petitioner’s commercial product embodies any of the additional features recited in claims 3–6, 12, 15, 20, and 21. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner’s commercial product meets certain limitations of claim 1 and claim 2, Patent Owner omits any discussion of the relationship of Petitioner’s commercial product to claims 3–6, 12, 15, 20, and 21. *See id.* at 71–76.

Having reviewed all of the parties’ arguments and evidence, we find Petitioner has shown unpatentability of claims 3–6, 12, 15, 20, and 21 over Capalik by a preponderance of the evidence. Pet. 35–40; PO Resp. 54, 68–76.

D. GROUND 2 – ALLEGED OBVIOUSNESS OVER CAPALIK AND GOEL

1. *Overview of Goel*

Goel “describe[s] the design, implementation, and evaluation of Forensix.” Ex. 1005, 1. “The goal of Forensix is to build a system that supports reliable reconstruction of all computer system activity for forensic purposes. Forensics is concerned with the capture, analysis and reconstruction of system activities in order to determine, post-facto, how or whether a machine was compromised.” *Id.*

“With Forensix, the *target system*’s kernel is instrumented with a logging facility.” Ex. 1005, 2. Goel observes that “a successful attack can only be caused by system-calls issued by processes running on the attacked system (provided the system is built correctly).” *Id.* Goel adds that “if *all* system-call activity is captured and can be attributed to users, processes or

connections, then it should be possible to accurately reconstruct *all* security incidents, immaterial of the type of attack.” *Id.*

In Goel’s system, “the backend periodically loads log data to a relational database.” Ex. 1005, 3. Goel explains that “Forensix logs within the kernel. In its current implementation, all activity across the system-call interface is captured and logged.” Goel shows system activity in Figure 2, which is reproduced below.

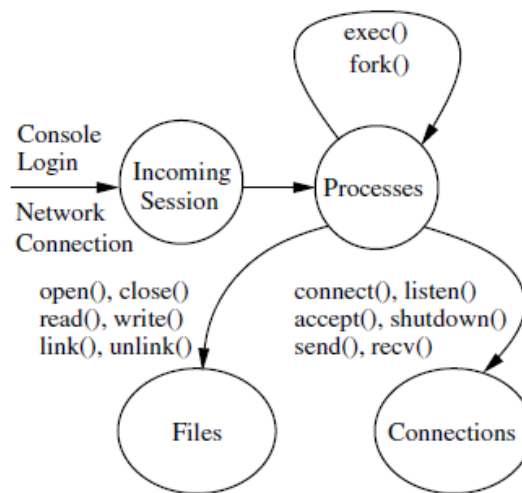


Figure 2. Relationships of system activities.

“Figure 2 shows a diagram of various system activities and their relationships.” Ex. 1005, 3.

Goel discloses that “incoming sessions, file accesses and outgoing connections are all associated with a process, while process creation via exec or fork is associated with the parent process.” Ex. 1005, 3. Goel adds that “each system-call trace record has an associated PID and a time-stamp that helps to construct the activity relationship.” *Id.*

2. Discussion

In Ground 2, “Petitioner relies on *Capalik’s* teachings as set forth in Ground 1” for many of the limitations of claims 1–6, 12, 14, 15, 20, and 21.

Pet. 40. Petitioner cites Goel as “teaching identifying and storing unauthorized activities wherein each activity includes an activity source, an activity target, and association,” as required by limitations 1(b), 20(b), and 21(b). *Id.*

Patent Owner argues that an ordinarily skilled artisan would not have combined Goel with Capalik. PO Resp. 55–59. According to Patent Owner, an ordinarily skilled artisan would have viewed Goel’s system as compromising certain aspects of Capalik’s system. *Id.*

Having reviewed all of the parties’ arguments and evidence, we determine Petitioner has shown unpatentability of claims 1, 3–6, 12, 14, 15, 20, and 21 over Capalik and Goel. Pet. 40–48; PO Resp. 55–59, 68–76; Reply 20–22, 29; Sur-Reply 15–17, 22–23. We determine that Petitioner has not shown unpatentability of claim 2 over Capalik and Goel. We turn now to a detailed discussion of the dispute regarding whether an ordinarily skilled artisan would have combined Capalik and Goel, followed by detailed discussions of the claim challenges.

a) Whether an Ordinarily Skilled Artisan Would Have Combined Capalik and Goel.

Petitioner argues that, in view of Goel, it would have been obvious to modify Capalik “to identify and store unauthorized activities including the activity source, activity target, and association of each activity.” Pet. 43–44. According Petitioner, an ordinarily skilled artisan would have had a number of reasons for doing so. *Id.* at 44–45. For example, Petitioner argues that the “modification applies the well-known computer security principle that gathering more detailed threat information provides improved threat analysis.” *Id.* at 44 (citing Ex. 1003 ¶ 79). Petitioner adds that the references describe using similar operating systems to process attack

information and store information related to unauthorized activities for the purpose of protecting against future attacks. *Id.* at 45 (citing Ex. 1003 ¶ 181; Ex. 1005, 2).

Patent Owner counters that recognized drawbacks would have dissuaded from the combination. PO Resp. 55–59. Arguing that Goel’s approach of gathering and storing attack information is more vulnerable to attacker detection than Capalik’s, Patent Owner contends that an ordinarily skilled artisan would not have implemented Goel’s system in Capalik. *Id.* For example, Patent Owner argues that “[a person of ordinary skill in the art] would not have been motivated to combine *Capalik* with *Goel* because *Goel* would have undermined *Capalik*’s requirement that activity logging be undetectable, rendering the system ‘not useful’ against sophisticated attacks.” *Id.* at 56 (citing Ex. 1004 ¶ 6). For example, Patent Owner argues that “[u]nlike *Capalik*, *Goel* does not disclose a decoy system and is not concerned with detectability.” *Id.* (citing Ex. 1005, 2). Patent Owner further argues that Goel’s system includes multiple telltales that would allow an attacker to detect Capalik’s monitoring. *Id.* at 57–58. For example, Patent Owner argues that Goel’s process uses kernel hooks and would slow Capalik’s machine, alleging that each of these would render Capalik’s monitoring detectable. *Id.* Patent Owner further argues that Goel touts performance improvements from monitoring directly inside the operating system, improvements that would not be realized when using a hypervisor like Capalik’s. PO Resp. 58–59 (citing Pet. 46; Ex. 2031 ¶¶ 77–79; Ex. 1005, 3).

In its Reply, Petitioner responds that its proposed combination involves modifying Capalik’s system to capture more data (sources, targets, and associations), not bodily incorporating all of Goel’s kernel hooks and

other features. Reply 21 (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). Petitioner also suggests that some risk of detection does not undermine a motivation to combine, explaining that even Patent Owner does not argue that Capalik’s system is entirely undetectable to attackers. Reply 21 n.6.

Patent Owner counters that “*In re Keller* is inapposite . . . the argument is simple: the combination results in detectability, and a [person of ordinary skill in the art] would not have done it.” Sur-Reply 17. Patent Owner argues that Petitioner’s Reply does not even dispute that the combination would have rendered Capalik detectable due to slower speed, as reflected in the Petition’s a “tradeoff between effectiveness and efficiency.” *Id.* at 15 (citing Pet. 43–46). Additionally, Patent Owner disputes Petitioner’s argument that the Petition did not suggest using Capalik’s kernel hooks. *Id.* at 16–17. And Patent Owner disagrees with Petitioner’s suggestion that some risk of detection is unavoidable. Sur-Reply 15 n.2. According to Patent Owner, the ’872 patent unequivocally conveys that its system is not vulnerable to detection. *Id.* (citing Ex. 1001, 7:43–50).

Based on our review of the complete record, we find Petitioner’s arguments and evidence to be more persuasive. Patent Owner does not dispute Petitioner’s argument and evidence that capturing detailed information like Goel’s activity sources, activity targets, and association was recognized as enhancing threat analysis. Pet. 44 (citing Ex. 1003 ¶ 79); *see* PO Resp. 55–59; Sur-Reply 15–17.

Additionally, contrary to Patent Owner’s suggestion, we find that the Petition does not propose incorporating Goel’s kernel hooks into Capalik’s system. *See* Pet. 41–46. Patent Owner contends that the Petition’s reference to modifying Capalik by “adding lines of code” suggests implementing the

kernel hooks. Sur-Reply 16. Patent Owner reasons that specific lines of code disclosed in Goel include kernel hooks. *Id.* Notwithstanding Patent Owner's assertion otherwise, this is an unpersuasive bodily incorporation argument, as the Petition never says an ordinarily skilled artisan would have used the exact lines of code from Goel in Capalik. Rather, the Petition says that an ordinarily skilled artisan would have had sufficient skill to implement straightforward code modifications to identify activity sources, targets, and associations:

a [person of ordinary skill in the art] would have understood that modifying *Capalik's* system (e.g., Linux-based) to additionally monitor, identify, and store each individual activity of an attack including "activity sources, activity targets, and associations" would have required straightforward modifications to programs/code instructions, which would have been well-within the skillset of a [person of ordinary skill in the art].

Pet. 46. Patent Owner argues that Petitioner does not explain how an ordinarily skilled artisan would have modified Capalik without using kernel hooks. Sur-Reply 17. But Patent Owner does not cite any evidence to counter Dr. Jakobsson's testimony that an ordinarily skilled artisan would have had the skill to apply Goel's general teaching of identifying sources, targets, and associations to Capalik's system. Ex. 1003 ¶ 182. On the whole, the evidence does not support Patent Owner's position that the combination would have required substantially increased detection risk.

Moreover, even if the combination would have somewhat increased detection risk, Petitioner persuades us that an ordinarily skilled artisan still would have had reason to combine the references teachings. Patent Owner's allegations of increased detection risk do not negate the undisputed evidence that the combination would have provided the advantage of improved threat analysis. Pet. 44 (citing Ex. 1003 ¶¶ 175–182). Ultimately, Patent Owner's

concerns rest on the cornerstone argument that Capalik has a “*requirement* that activity logging be undetectable.” PO Resp. 56 (emphasis added) (citing Ex. 1004 ¶ 6). This exaggerates Capalik’s disclosure. Although the cited paragraph suggests that certain systems unfortunately may be detectable by some users, it does not convey that it is a requirement for the system to be categorically undetectable. *See* Ex. 1004 ¶ 6.⁸

In sum, Petitioner persuades us by a preponderance of the evidence that it would have been obvious to modify Capalik “to identify and store unauthorized activities including the activity source, activity target, and association of each activity.” Pet. 41–46; PO Resp. 55–59; Reply 20–22; Sur-Reply 15–17.

b) Claim 1

Having argued that Capalik teaches all of claim 1’s limitations (Pet. 13–34), Petitioner argues that Goel supplements Capalik’s disclosures with respect to activity sources, targets, and associations:

[t]o the extent Patent Owner disputes that *Capalik* identifies and stores a source, target, and association for each of the individual activities of an attack, *Goel* demonstrates that it was known in the art to identify and store each of the individual activities of an attack (including the activity source, target, and association) to generate signatures indicative of the activities for forensic analysis.

Pet. 40. Patent Owner argues that “Ground 2 fails for the same reasons as Ground 1” because Petitioner “relies entirely on its

⁸ Similarly, we do not agree with Patent Owner’s assertion that the ’872 patent discloses its monitoring is entirely undetectable. Sur-Reply 15 n.2 (citing Ex. 1001, 7:43–50). The cited passage only says “it is *difficult* for an attacker accessing the decoy operating system 112 to determine whether the decoy operating system 112 is being monitored.” Ex. 1001, 7:47–50 (emphasis added).

Ground 1 analysis of Capalik for the ‘data structure’ of limitation 1[C] as well as all of limitation 1[D].” PO Resp. 54. As discussed above in Section III.D.2.a), Patent Owner further argues that an ordinarily skilled artisan would not have combined Goel’s disclosure with Capalik’s. *Id.* at 55–59.

As discussed above in Section III.C.2.a), Petitioner shows by a preponderance of the evidence that Capalik teaches all of claim 1’s limitations. Pet. 13–34. Additionally, Petitioner shows that, in combination, Capalik and Goel teach all of claim 1’s limitations. Pet. 40–43. And, as discussed above in Section III.D.2.a), Petitioner shows by a preponderance of the evidence that it would have been obvious to combine Capalik and Goel. Pet. 43–46.

Regarding objective indicia of non-obviousness, as discussed above in Section III.C.2.a).(6), Patent Owner does not show nexus for claim 1 because (1) claim 1 is not novel over Capalik and (2) Patent Owner does not sufficiently show that Petitioner’s commercial product embodies claim 1.

In sum, Petitioner shows unpatentability of claim 1 over Capalik and Goel by a preponderance of the evidence.

c) Claim 2

In Ground 2, Petitioner relies on its Ground 1 arguments for claim 2. Pet. 46. As discussed above in Section III.C.2.b), Petitioner does not show unpatentability of claim 2 in Ground 1. Accordingly, Petitioner does not show unpatentability of claim 2 in Ground 2.

d) Claims 3–6, 12, 14, 15, 20, and 21

In Ground 2, Petitioner relies on its Ground 1 arguments for most limitations of claims 3–6, 12, 14, 15, 20, and 21, citing Goel for certain

limitations in claim 14. Pet. 46–48. Patent Owner reiterates its position that Capalik does not teach certain limitations of claim 1. PO Resp. 54. Patent Owner also argues that an ordinarily skilled artisan would not have combined Capalik and Goel. *Id.* at 55–59.

Having reviewed all of the parties’ arguments and evidence, we find that Petitioner shows by a preponderance of the evidence that, in combination, Capalik and Goel teach all limitations of claims 3–6, 12, 14, 15, 20, and 21. Additionally, as discussed above in Section III.D.2.a), Petitioner shows by a preponderance of the evidence that it would have been obvious to combine Capalik and Goel.

Regarding objective indicia of obviousness, Patent Owner does not show nexus for any of claims 3–6, 12, 14, 15, 20, and 21. As explained above in Section III.C.3, Patent Owner does not show that Petitioner’s commercial product embodies any of claims 3–6, 12, 14, 15, 20, and 21. *See* PO Resp. 71–76.

In sum, Petitioner shows unpatentability of claims 3–6, 12, 14, 15, 20, and 21 over Capalik and Goel by a preponderance of the evidence.

E. GROUND 3 – ALLEGED OBVIOUSNESS OVER CAPALIK, GOEL, AND KING

1. *Overview of King*

King notes that “[m]odern computer systems are under attack.” Ex. 1006, 1.⁹ With this background, King “propose[s] using operating-system-level(OS-level) information-flow graphs to highlight the activities of an attacker.” *Id.* at 3. King notes that “[i]nformation-flow graphs can be used to describe behavior on a computer system”:

⁹ We cite to King’s native page numbers, rather than the page numbers added at the lower righthand corners.

A graph of *known-good* behavior defines how a service interacts with the system and how information flows between components, any deviations from this graph of known-good behavior may indicate potentially suspicious activity. In addition, a graph of *known-bad* behavior defines known malicious activities, acting as a signature for an intrusion detection system.

Ex. 1006, 64.

King discloses that its “EventLogger keeps track of a process from the time it is created by a fork or clone system call to the point where it exits.”

Ex. 1006, 12. King elaborates that “EventLogger logs events at runtime that induce dependency relationships between objects, i.e. events in which one object affects the state of another object. These events are the links that allow us to deduce timelines of events connecting various objects together.”

Id. at 13.

King “save[s] enough information to build an information-flow graph that depicts the dependency relationships between all objects seen over [an] execution.” Ex. 1006, 16. King does so “[b]y logging objects and dependency-causing events during runtime.” *Id.*

King also discloses that a part of its system called GraphGen builds a dependency graph “of all objects and events that causally affect . . . the state of the detection point (backward information flow) or are causally affected by the state of the detection point (forward information flow).” Ex. 1006, 17. King shows an exemplary dependency graph in Figures 3.2(a), 3.2(b), and 3.2(c), which are reproduced below.

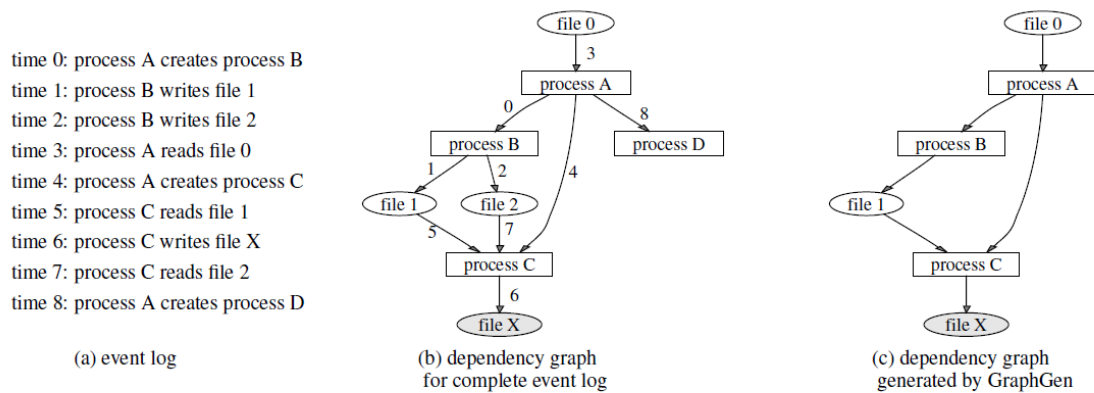


Figure 3.2(a) shows an event log. Ex. 1006, 19. Figure 3.2(b) shows a “dependency graph for complete event log.” *Id.* And Figure 3.2(c) shows Figure 3.2(c) shows a “dependency graph generated by GraphGen.” *Id.*

2. Discussion

In Ground 3, Petitioner builds from Grounds 1 and 2, arguing the following:

As explained above with respect to [limitations 1(b) and 1(c)], *Capalik* (Ground 1) or *Capalik-Goel* (Ground 2) teaches identifying a plurality of activities (including activity sources, activity targets, and associations) performed at the computer system, and retaining detailed forensic data that can be used to generate signatures indicative of the activities.”

Pet. 48. Petitioner cites King for its GraphGen disclosures to address limitations added by claims 7–11, 14, 16, 18, and 19. *Id.* at 48–66.

Petitioner argues that an ordinarily skilled artisan would have been motivated “to modify *Capalik/Capalik-Goel* per *King* to display a subset of the stored activities, including activity sources, activity targets, and associations for each activity.” *Id.* at 52. Petitioner reasons that an ordinarily skilled artisan would have recognized that such a combination would have enhanced threat analysis, such as by displaying information that

“would have allowed an administrator to readily identify the attack path.”
Id. at 52–53.

Patent Owner reiterates its position that Grounds 1 and 2 fail, asserting that Ground 3 fails for the same reasons. PO Resp. 59. Patent Owner separately argues that Petitioner does not persuasively address the limitations of claims 8, 16, and 19. *Id.* at 59–67.

Having reviewed all of the parties’ arguments and evidence, we find that Petitioner has shown unpatentability of claims 7, 9–11, 16, 18, and 19 over Capalik, Goel, and King. Pet. 48–54, 56–66; PO Resp. 59, 61–66; Reply 23–25; Sur-Reply 20–22. We find that Petitioner has not shown unpatentability of claim 8 over Capalik, Goel, and King. Pet. 49–56; PO Resp. 59–61; Reply 22–23; Sur-Reply 17–18. We turn now to detailed discussions of the claim challenges.

a) Claims 7, 9–11, 14, and 18

Petitioner argues that, in combination, Capalik, Goel, and King render obvious claims 7, 9–11, 14, and 18. Pet. 48–54, 56–62, 64. Patent Owner contests this challenge by citing its arguments that Petitioner failed to show unpatentability of claim 1 in Grounds 1 and 2. PO Resp. 59. This argument is unpersuasive because, as discussed above in Sections III.C.2.a) and III.D.2.a), b), Petitioner has shown unpatentability of claim 1 in Grounds 1 and 2.

Regarding objective indicia, Patent Owner has not shown a nexus for any of claims 7, 9–11, 14, and 18. Patent Owner does not show Petitioner’s commercial product embodies any of claims 7, 9–11, 14, and 18. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner’s commercial product meets certain limitations of claim 1 and claim 2, Patent

Owner omits any discussion of the relationship of Petitioner's commercial product to any of claims 7, 9–11, 14, and 18. *See id.* at 71–76.

In sum, we determine Petitioner has shown unpatentability of claims 7, 9–11, 14, and 18 by a preponderance of the evidence. Pet. 48–54, 56–62, 64; PO Resp. 59.

b) Claim 8

Adding to claim 7's recitation of "displaying at least a subset of the stored activities," claim 8 recites "the displaying includes visually distinguishing at least a subset of the associations." Ex. 1001, 20:10–13. Petitioner contends that King teaches this in connection with its Figures 3.2(b) and 3.2(c). Pet. 54–56; Reply 22–23. Petitioner argues that King teaches identifying malignant and benign associations when doing the analysis reflected by Figure 3.2(b). Pet. 49–51, 55; Reply 22. When explaining this, Petitioner annotates King's Figure 3.2(b) with green and yellow annotations to identify malignant and benign associations. Pet. 55; Reply 22. Petitioner also argues that King teaches displaying the graph shown in Figure 3.2(c), which shows the identified malignant associations but does not show the identified benign associations. Pet. 55; Reply 22. Because King teaches displaying only a subset of associations (the malignant associations), Petitioner contends that King teaches visually distinguishing the displayed associations. Pet. 55; Reply 22.

In response, Patent Owner argues that neither King's Figure 3.2(b) nor King's Figure 3.2(c) teaches claim 8. PO Resp. 59–61; Sur-Reply 17–19. Patent Owner argues that Figure 3.2(b) does not teach claim 8 because King does not teach displaying Figure 3.2(b). PO Resp. 59–60; Sur-Reply 19. Patent Owner argues that King's Figure 3.2(c) does not teach claim 8

because “[m]erely displaying a subset does not ‘visually distinguish’ the subset.” PO Resp. 60.

Weighing the parties’ arguments and evidence, we find that Petitioner has not carried its burden. We agree with Patent Owner that Petitioner does not persuasively rebut Patent Owner’s contention that King does not teach displaying Figure 3.2(b) (or Petitioner’s colored annotations). PO Resp. 60; Reply 22–23; Sur-Reply 19. Indeed, Petitioner acknowledged at oral argument that “what we have relied on really is . . . figure 3.2C from King. This is what’s referred to as a filtered dependency graph that is generated by King.” Tr. 35:25–36:3.

Accordingly, Petitioner’s position that King teaches claim 8 rests on the argument that King teaches displaying only malicious associations in Figure 3.2(c). Reply 22 (“By displaying *only* malignant associations in its filtered graph, King is visually distinguishing the subset of associations that are malignant.”). And that argument rests on Petitioner’s position that claim 8’s “visually distinguishing at least a subset of the associations” encompasses displaying only a subset of associations, which is unsupported for the reasons explained above in Section III.B.3. Accordingly, Petitioner does not show by a preponderance of the evidence that the prior art teaches claim 8.

c) Claim 16

Claim 16 depends from claim 1 and further recites the following:
determining an activity status for the stored events, the activity status comprising one of:

a complete status representing that a source of unauthorized activities is identified, and each activity and target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more association.

Ex. 1001, 20:48–54.

Citing King’s disclosures associated with Figure 3.2(c), Petitioner argues that the combination of Capalik, Goel, and King teaches claim 16. Pet. 62–64. Petitioner notes that the ’872 patent’s “[Figure] 4A illustrates an incomplete status in which at least one target is not associated with a source,” whereas “an example of a complete status is depicted in [Figure] 4D, wherein ‘each activity is associated with the source, packet stream 304 through one or more associations.’” *Id.* at 62 (quoting Ex. 1001, 17:23–28). Petitioner argues that, like the ’872 patent’s Figure 4D, King’s Figure 3.2(c) shows associations between sources and targets, thereby “illustrat[ing] a complete activity status for an attack.” *Id.* at 63–64 (citing Ex. 1006, Fig. 3.2; Ex. 1003 ¶¶ 229–233).

Patent Owner counters that “mere depiction of a graph” does not satisfy claim 16. PO Resp. 62. Instead, the ’872 patent “explicitly [discloses] determining an activity status as a step *wholly separate* from graphical display,” Patent Owner argues. *Id.* at 62–64 (citing Ex. 1001, 12:45–67, Figs. 5A, 6B, 6C). Patent Owner also argues that “[a] ‘filtered’ graph in King is merely the result of excluding from the graph data deemed irrelevant to the chosen detection point; it is not a determination whether each target in the stored activities are associated to a source as required by claim 16.” *Id.* at 62.

Petitioner responds that Patent Owner “mischaracteriz[es] Petitioner’s theory as based solely on the display of Fig. 3.2(c), rather than the process leading to its creation.” Reply 24. Petitioner argues that King supports its

position because “King’s filtered dependency graph Fig 3.2(c) is created *only after* the system has determined a complete status, identifying (1) a source of unauthorized activities and (2) associations to every activity target.” *Id.* at 23 (citing Pet. 63–64; Ex. 1003 ¶ 231).

In response, Patent Owner argues that Petitioner’s case is procedurally and substantively deficient. Sur-Reply 20–21. Regarding procedure, Patent Owner first argues that the Reply improperly raises a new argument by asserting that King displays the Figure 3.2(c) graph only after determining an activity status. *Id.* at 20. Patent Owner then argues that “[t]o the extent [Petitioner] attempts to incorporate paragraph 231 of its expert’s declaration into the Petition (*see* Reply at 23 (citing Ex. 1003, ¶231)), such incorporation would be improper.” *Id.* (citing 37 C.F.R. § 42.6(a)(3)). Regarding substance, Patent Owner argues that “King merely creates a graph from the stored data, prunes it, and displays the pruned graph. The claim requires a binary status determination—complete or incomplete—that King never makes.” *Id.* (citing POR 62).

On both the procedural and substantive issues, Petitioner has the better position. In concert with its argument that “[Figure] 3.2(c) illustrates a complete activity status for an attack,” the Petition explained that “*King’s system* identifies a source of unauthorized activities (e.g., file 0) and that source’s relation to every activity target (e.g., process B, file 1, process C, file X) through one or more identified associations.” Pet. 63 (emphasis added). Although the significance of this could have been explained more clearly, this argument reasonably conveys that the process leading up to displaying Figure 3.2(c) involves King determining a complete activity status. In support of this position, the Petition cited paragraph 231 of Dr. Jakobsson’s first declaration, along with only four other paragraphs of

the first declaration. We find this is an example of relying on a reasonable volume of witness testimony to further support the argument presented in the Petition, not an improper incorporation of argument from one document into another.

Regarding the substance, we find Dr. Jakobsson’s testimony persuasive, as it explains logically why it would have been understood from King that the *process leading up to* displaying the dependency graph involves determining a complete status for the stored activities. *E.g.*, Ex. 1003 ¶¶ 230–231. This prevails over Patent Owner’s counter that King lacks any express discussion of “a binary status determination—complete or incomplete.” Sur-Reply 20; *See Preda*, 401 F.2d at 826.

Regarding objective indicia, Patent Owner has not shown a nexus for claim 16. Patent Owner does not show Petitioner’s commercial product embodies claim 16. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner’s commercial product meets certain limitations of claim 1 and claim 2, Patent Owner omits any discussion of the relationship of Petitioner’s commercial product to claim 16. *See id.* at 71–76.

Having reviewed all of the parties’ arguments and evidence, we find Petitioner has shown unpatentability of claim 16 by a preponderance of the evidence. Pet. 62–64; PO Resp. 61–64; Reply 23–24; Sur-Reply 20–21.

d) Claim 19

Claim 19 depends from claim 1 and recites “wherein the association includes a type that represents whether or not the activity source has modified the activity target to perform the unauthorized activities.” Ex. 1001, 21:1–4. Petitioner argues that the combination of Capalik, Goel, and King “teaches identifying a type of the association between the activity source and the activity target, as depicted in *King’s* dependency graph

generated by GraphGen.” Pet. 64 (citing Ex. 1006, Fig. 3.2; Ex. 1003 ¶ 235). Petitioner explains that King generates the graph in Figure 3.2(c) by “detecting a suspicious object (e.g., file X having the wrong contents at time 10),” analyzing the attack activity, and “remov[ing] any associations that did not contribute (directly or indirectly) to the unauthorized activity identified at time 10” from Figure 3.2(b)’s information flow graph. *Id.* at 65 (citing Ex. 1006, 18–19; Ex. 1003 235). Petitioner concludes that an ordinarily skilled artisan “would have understood that the associations remaining after this filtering are of a type that represents a source modifying its target to perform unauthorized activities either directly (e.g., writing incorrect content into file X) or indirectly (e.g., causing a subsequent source to write incorrect content into file X).” *Id.* at 65–66.

Patent Owner argues that Petitioner’s challenge includes a “failure doom[ing] Ground 3 for claim 19.” PO Resp. 66. Specifically, Patent Owner faults Petitioner for “not even attempt[ing] to address how the Ground 3 combinations disclose storing a ‘data structure’ that identifies the association ‘type’ required by claim 19.” *Id.* Patent Owner explains that claim 19 depends from claim 1, which recites “storing in the memory a data structure that identifies . . . the associations for the plurality of activities.” *Id.* at 65. And Patent Owner notes that the ’872 patent’s Figure 5A shows a data structure that stores an association type. *Id.* at 65–66.

Weighing the parties’ arguments and evidence, we find Petitioner’s more persuasive. As explained above in Section III.C.2.a).(4), Patent Owner does not persuasively rebut Petitioner’s arguments that Capalik teaches to an ordinarily skilled artisan claim 1’s “storing in memory a data structure that identifies . . . the associations.” Pet. 22–30, 64–65; PO Resp. 14–18, 64–67; Reply 4–9, 24–25; Sur-Reply 21–22. Nor does Patent Owner persuasively

rebut Petitioner’s arguments and evidence that, in combination, Capalik, Goel, and King teach to an ordinarily skilled artisan that the associations have identified types. Pet. 64–65; PO Resp. 64–67; Reply 24–25; Sur-Reply 21–22.

That leaves Patent Owner’s argument that the prior art does not teach storing the association’s type in a data structure like that of claim 1. PO Resp. 65–66; Sur-Reply 21. This argument is not commensurate in scope with the claim. As Patent Owner observes, claim 1 requires that the data “identifies . . . the associations.” Ex. 1001, 19:50–53. Patent Owner appears to argue that this requires storing the association’s type. *See* Sur-Reply 21 (“This ‘type’ must be part of the association that is stored in the data structure required by claim 1.”). But Patent Owner does not provide persuasive reasoning that identifying an association would require storing the association’s type. PO Resp. 64–67; Sur-Reply 21–22.

Additionally, claims 1 and 19 do not recite that the data structure stores any particular attribute of an association. Ex. 1001, 19:50–52, 21:1–4. Claim 1 recites that the data structure identifies associations, not that it stores any particular attribute of the associations. *Id.* at 19:50–52. Claim 19 recites that the association has a particular attribute, not that the data structure stores that attribute. *Id.* at 21:1–4.

Additionally, although Patent Owner is correct that the ’872 patent’s Specification discloses storing associations’ types in a data structure, Patent Owner does not persuade us to incorporate this limitation into the claim. PO Resp. 65–66; *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (“Though understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not part of the claim.”). Even when

discussing the exemplary data structures in Figure 5A and 5B, the '872 patent expressly describes storage of association type as “optional.”

Ex. 1001, 13:39–42, 13:66–14:4.

Regarding objective indicia, Patent Owner has not shown a nexus for claim 19. Patent Owner does not show Petitioner’s commercial product embodies claim 19. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner’s commercial product meets certain limitations of claim 1 and claim 2, Patent Owner omits any discussion of the relationship of Petitioner’s commercial product to claim 19. *See id.* at 71–76.

Having reviewed all of the parties’ arguments and evidence, we find Petitioner has shown unpatentability of claim 19 by a preponderance of the evidence. Pet. 64–66; PO Resp. 64–67; Reply 24–25; Sur-Reply 21–22.

F. GROUND 4 – ALLEGED OBVIOUSNESS OVER CAPALIK, GOEL, AND PIKE

1. *Overview of Pike*

Pike “relates generally to computational systems and, more particularly, to security techniques for identifying and (in some cases) interdicting information system intrusions.” Ex. 1007, 1:8–11. Pike discloses that computational systems may interact with external computers, which may be untrusted. *Id.* at 4:62–65.

In such interactions, “input streams may contain (or encode) subsequences suitable for use in an exploit.” Ex. 1007, 6:51–54. Pike discloses “a strategy of identifying subsequences of interest and instrumenting a computational system to detect their inappropriate use.” *Id.* at 6:60–62. Pike discloses “us[ing] any of a variety of techniques, including setting a relevant no-execute bit, unmapping the corresponding memory page, marking a page as non-readable or non-writable, truncating a

code segment, truncating a data segment or setting a breakpoint.”

Id. at 8:65–9:5.

2. Discussion

In Ground 4, Petitioner challenges claim 13 based on *Capalik*, *Goel*, and *Pike*. Ground 4 builds from Grounds 1 and 2, arguing that “*Capalik* (Ground 1) or *Capalik-Goel* (Ground 2) teaches Claims 1, 12.” Pet. 66. Petitioner cites *Pike* to address claim 13’s recitation of “wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.” *E.g., id.* at 66–67. Petitioner asserts that “[t]he ’872 Patent describes identifying activity sources that request to access a portion of memory that is set as non-executable can be achieved by data execution prevention (DEP) mechanisms, including using a non-executable bit.” *Id.* at 67. Petitioner contends that “*Pike* teaches one such DEP mechanism.” *Id.*

Patent Owner argues that Ground 4 both fails to cure the deficiencies in Ground 1 and fails to persuasively address claim 13’s added limitations. PO Resp. 67–68. Patent Owner notes that claim 13 requires “identifying activity sources that request to access a portion of memory that is set as non-executable.” PO Resp. 67. In contrast, “*Pike* is only concerned with scenarios where ‘the potentially dangerous address is *accessed*,’” Patent Owner argues. *Id.* (quoting with emphasis Ex. 1007, 8:65–67). Patent Owner asserts that “[a]t best, *Pike* identifies a source that accesses such memory, identifying an actual intrusion but missing sources that merely request such access. [Petitioner] ignores this difference between *Pike* and claim 13.” *Id.* at 68.

Petitioner counters that Pike discloses the same processes that the '872 patent discloses using for detecting attempted access. Reply 26. In particular, Petitioner cites Dr. Jakobsson's testimony about Pike "setting a relevant no-execute bit that triggers an exception." Ex. 1003 ¶ 240; Reply 26. According to Petitioner, Pike teaches the same process that the '872 patent discloses for implementing claim 13's limitations:

Pike teaches a process expressly identified in the '872 Patent as satisfying the claimed concept. Specifically, the patent teaches that the limitation "can be achieved by data execution prevention (DEP) mechanisms[,] . . . e.g., using a non-executable bit in respective page table entries[] and generat[ing] an exception when there is an attempt to execute an instruction that is set as non-executable."

Reply 26 (quoting Ex. 1001, 16:8–20).

In response, Patent Owner suggests that Petitioner fails to support its contention that Pike teaches the same process that the '872 patent discloses for detecting access *requests*. Sur-Reply 22. Patent Owner argues that "Pike does not use the term 'data execution prevention' or 'DEP.'" *Id.* Patent Owner further argues that "the Petition cites to Pike's disclosure of configuring systems 'to trigger an action if and when memory 295 identified by the potentially dangerous address *is accessed*.'" *Id.* (quoting with emphasis Ex. 1007, 8:65–67).

Based on our review of the full record, we find Petitioner's argument and evidence to be persuasive. Dr. Jakobsson identifies significant similarity between Pike's process and the '872 patent's description of known ways to identify unauthorized access requests. *E.g.*, Ex. 1003 ¶¶ 238–240. For example, Dr. Jakobsson notes that Pike "teaches setting a relevant no-execute bit that triggers an exception." Ex. 1003 ¶ 240 (citing Ex. 1007, 8:65–9:12, 9:24–10:1, 12:58–13:22). This closely resembles the '872

patent's disclosed process of identifying unauthorized activities by "setting one or more portions of the memory as non-executable . . . and generat[ing] an exception when there is an attempt to execute an instruction that is set as non-executable." Ex. 1001, 16:15–20. This is sufficient to show that an ordinarily skilled artisan would have understood from Pike's disclosure that its process would detect access requests, as required by claim 13.

Patent Owner unpersuasively counters that Pike does not use the same moniker that the '872 patent uses for its process, arguing that "Pike does not use the term 'data execution prevention' or 'DEP.'" Sur-Reply 22. Patent Owner also cites Dr. Stavrou's testimony as supporting its position. *Id.* (citing Ex. 2031 ¶¶ 95–96). Dr. Stavrou's testimony focuses on the fact that Pike does not expressly disclose identifying access requests but teaches identifying when memory actually has been accessed. Ex. 2031 ¶¶ 95–96. Merely because Pike does not expressly discuss identifying access requests, that does not persuasively rebut Petitioner's evidence that an ordinarily skilled artisan would have understood that Pike's process would have identified access requests. Accordingly, Petitioner shows by a preponderance of the evidence that "a [person of ordinary skill in the art] would have understood that *Pike* teaches identifying activity sources affected by unauthorized activities that request to access a portion of memory that is set as non-executable, as claimed." Pet. 68.

Regarding objective indicia, Patent Owner has not shown a nexus for claim 13. Patent Owner does not show Petitioner's commercial product embodies claim 13. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner's commercial product meets certain limitations of claim 1 and claim 2, Patent Owner omits any discussion of the relationship of Petitioner's commercial product to claim 13. *See id.* at 71–76.

Having reviewed all of the parties' arguments and evidence, we find Petitioner has shown unpatentability of claim 13 by a preponderance of the evidence. Pet. 64–69; PO Resp. 67–68; Reply 25–26; Sur-Reply 22.

G. GROUND 5 – ALLEGED OBVIOUSNESS OVER CAPALIK, GOEL, AND FARLEY

1. *Overview of Farley*

Farley relates to security of computer systems. Ex. 1008, 1:16–17. Farley discusses an embodiment in connection with Figure 2, which is reproduced below.

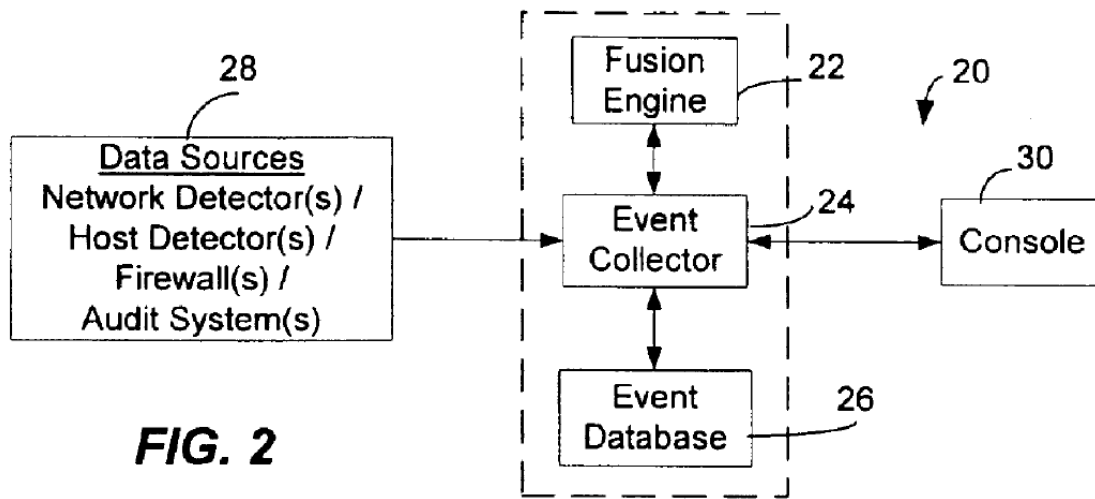


Figure 2 “is a functional block diagram” showing “[s]ystem 20 for managing security information collected from one or more data sources.”

Ex. 1008, 5:23–24, 9:31–33.

Security system 20 includes fusion engine 22, event collector 24, event database 26, data sources 28, and console 30. Ex. 1008, 9:33–34, 9:43–47. Data sources 28 “provide the event collector 24 with various types of information as it may relate to the network, host or single computer being monitored by the security management system 20.” *Id.* at 9:66–10:3. Event collector 24 sends “information received from the data sources 28 to the

fusion engine 22.” *Id.* at 10:13–15. “The fusion engine assembles or ‘fuses’ the raw events or information received from the event collector 24.”

Id. at 10:20–22. Figure 5C, which is reproduced below, shows “an exemplary raw event that has been processed by the CoBRA processor of the fusion engine.” *Id.* at 5:38–40.

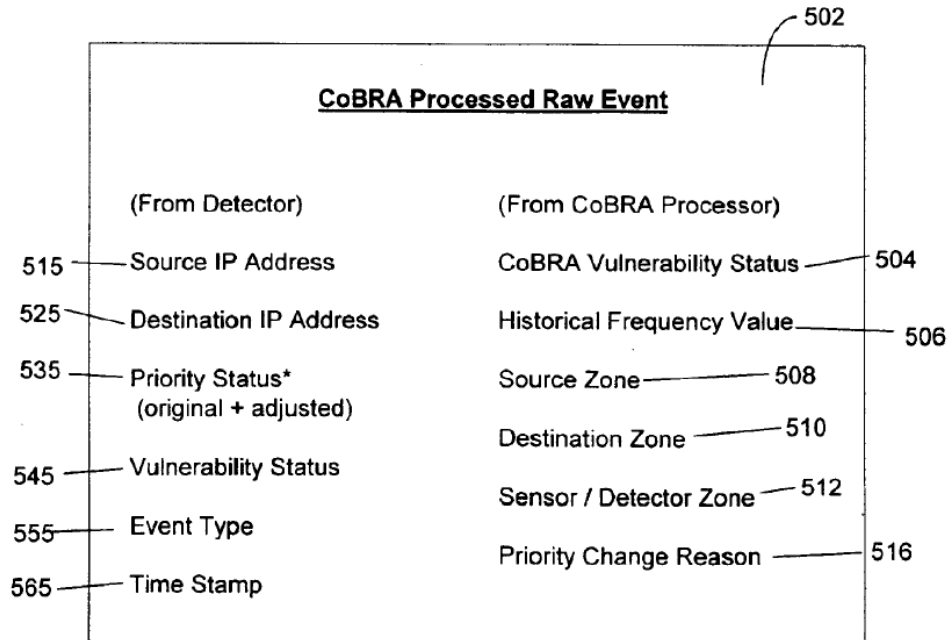


FIG. 5C

Figure 5C shows “a CoBRA-(Context Based Risk Adjustment) processed raw event,” specifically, CoBRA-processed raw event 502.

Ex. 1008, 12:13–15.

Farley explains that CoBRA-processed raw event includes “detector assigned parameters” in combination with “CoBRA-processed parameters,” which may include the following:

a CoBRA-assigned vulnerability value 504; a CoBRA-assigned historical frequency value 506; a CoBRA assigned source Zone value 508; a CoBRA-assigned destination Zone value 510; a CoBRA-assigned sensor Zone value 512; a CoBRA-assigned original priority status 514; and a priority change reason 516 text

string comprising a reason why the priority of the raw event was adjusted (if adjusted).

Ex. 1008, 12:15–25.

2. Discussion

In Ground 5, Petitioner builds from Grounds 2 and 3, arguing that “[a]s explained above, *Capalik* (Ground 1) or *Capalik-Goel* (Ground 2) teaches Claim 1.” Pet. 69. Petitioner cites Farley to address claim 17’s recitation of the further step of “determining an activity level representing a frequency of unauthorized activities on the first computer system during a predefined time interval.” *Id.* at 69–74. According to Petitioner, “a [person of ordinary skill in the art] would have understood that *Farley*’s ‘historical event frequency value’ is an activity level representing a frequency of unauthorized activities on a computer system during a predefined interval.” *Id.* at 72. Petitioner argues that “[a person of ordinary skill in the art] would have been motivated and found it obvious to modify *Capalik/Capalik-Goel* per *Farley* such that *Capalik-Farley/Capalik-Goel-Farley* would have determined an activity level (i.e., historical frequency value) representing a frequency of unauthorized activities on the computer system.” *Id.*

Patent Owner contests this challenge by citing its arguments that Petitioner failed to show unpatentability of claim 1 in Grounds 1 and 2. PO Resp. 68. This argument is unpersuasive because, as discussed above in Sections III.C.2.a) and III.D.2.a), b), Petitioner has shown unpatentability of claim 1 in Grounds 1 and 2.

Regarding objective indicia, Patent Owner has not shown a nexus for claim 17. Patent Owner does not show Petitioner’s commercial product embodies claim 17. *See* PO Resp. 68–76. Indeed, whereas Patent Owner suggests that Petitioner’s commercial product meets certain limitations of

claim 1 and claim 2, Patent Owner omits any discussion of the relationship of Petitioner's commercial product to claims 17. *See id.* at 71–76.

Having reviewed all of the parties' arguments and evidence, we find that Petitioner has shown unpatentability of claim 17 over Capalik, Goel, and Farley. Pet. 69–74; PO Resp. 68.

IV. CONCLUSION

Petitioner has shown by a preponderance of the evidence that the '872 patent's claims claim 1, 3–7, and 9–21 are unpatentable, but has not shown that either of claim 2 or claim 8 is unpatentable.

Claims	35 U.S.C. §	References/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–6, 12, 15, 20, 21	103	Capalik	1, 3–6, 12, 15, 20, 21	2
1–6, 12, 14, 15, 20, 21	103	Capalik, Goel	1, 3–6, 12, 14, 15, 20, 21	2
7–11, 14, 16, 18, 19	103	Capalik, Goel, King	7, 9–11, 14, 16, 18, 19	8
13	103	Capalik, Goel, Pike	13	
17	103	Capalik, Goel, Farley	17	
Overall Outcome			1, 3–7, 9–21 ¹⁰	2, 8

¹⁰ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding, 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

V. ORDER

It is:

ORDERED that claims 1, 3–7, and 9–21 of U.S. Patent No. 9,954,872 B2 have been shown unpatentable;

FURTHER ORDERED that claims 2 and 8 of U.S. Patent No. 9,954,872 B2 have not been shown unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2025-00070
Patent 9,954,872 B2

FOR PETITIONER:

Paul Hart
Adam Seitz
ERISE IP, P.A.
paul.hart@eriseip.com
adam.seitz@eriseip.com

FOR PATENT OWNER:

Srinivas Giriraj Pathmanaban
Daniel Todd
Steven Peters
CLEARY GOTTLEIB STEEN & HAMILTON LLP
gpathmanaban@cgsh.com
dtodd@cgsh.com
speters@cgsh.com
maofiling@cgsh.com

Raghav Bajaj
LATHAM & WATKINS LLP
raghav.bajaj@lw.com