

Filed on behalf of: GoSecure, Inc.

Entered: April 23, 2026

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

Case IPR2025-00070
Patent 9,954,872

PATENT OWNER'S SUR-REPLY TO PETITIONER'S REPLY

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Ground 1	1
A.	Limitation 1[c].....	1
1.	The '872 patent does not equate “forensic data” to the claimed “data structure”	2
2.	The '872 patent does not demonstrate that <i>Capalik's</i> “forensic data” identifies activity sources, targets, and associations.	7
B.	Limitation 1(d)	9
C.	Claim 2	11
III.	Ground 2 – Capalik / Goel.....	15
IV.	Ground 3	17
A.	Claim 8.	17
B.	Claim 16.	20
C.	Claim 19.	21
V.	Ground 4 (Claim 13).....	22
VI.	Objective indicia.....	22
VII.	Conclusion	23

TABLE OF AUTHORITIES

	Page(s)
Federal Cases	
<i>Apple Inc. v. Andrea Elecs. Corp.</i> , 949 F.3d 697 (Fed. Cir. 2020)	9
<i>Chef America, Inc. v. Lamb-Weston, Inc.</i> , 358 F.3d 1371 (Fed. Cir. 2004)	15
<i>CrowdStrike, Inc. v. GoSecure, Inc.</i> , IPR2025-00067, Paper 13 (PTAB May 6, 2025)	13

Exhibit List

Exhibit	Description
2001	Declaration of Joseph Greenfield, Ph. D.
2002	<i>Curriculum vitae</i> of Joseph Greenfield, Ph. D.
2003	Cisco ISP 4200 Series Sensors Datasheet
2004	Snort and Snort Rules Explained, available at https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/snort-rules/
2005	<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2023-00852, Paper 18 (PTAB Nov. 9. 2023)
2006	Declaration of June Ann Munford, <i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2023-00852, Ex. 1012
2007	<i>SalesForce.com, Inc. v. WSOU Investments, LLC</i> , IPR2022-00357, Paper 12 (PTAB July 13, 2022)
2008	<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2022-01566, Paper 13 (PTAB May 31, 2023)
2009	Cisco – Upgrading, Downgrading, and Installing System Images, available at https://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliimage.html#wp1091978
2010	RESERVED
2011	Univ. of Mich. Libr., Catalog-Library Search: <i>computer intrusions</i> , <a computer+intrusions\"&utm_source='lib-use-search-page"' href="https://search.lib.umich.edu/catalog?query=\">https://search.lib.umich.edu/catalog?query=\"computer+intrusions\"&utm_source=lib-use-search-page (last visited Mar. 26, 2025, 9:24 AM)

Exhibit	Description
2012	<i>PR Newswire</i> , “CounterTack Appoints Two New Board Members,” https://www.prnewswire.com/news-releases/countertack-appoints-two-new-board-members-135086178.html (last accessed June 16, 2025)
2013	Wayback Machine archive of <i>Security Battlefield</i> , George Kurtz, “CrowdStrike launches in stealth-mode with \$26 million Series A round led by Warburg Pincus,” Feb. 22, 2012, archived January 26, 2013, https://web.archive.org/web/20130126085516/http://www.georgekurtz.com/2012_02_01_archive.html (last accessed June 16, 2025)
2014	LinkedIn, <i>Jeremy Gould – Experience</i> , https://www.linkedin.com/in/jb0nz/details/experience/ (last accessed June 17, 2025)
2015	Wayback Machine archive of <i>CrowdStrike</i> , “Technology,” archived July 7, 2013, https://web.archive.org/web/20130707085243/http://www.crowdstrike.com/technology/index.html (last accessed June 20, 2025)
2016	Wayback Machine archive of <i>CrowdStrike</i> , “Next-Generation Threat Protection,” archived November 17, 2013, https://web.archive.org/web/20131127114229/http://www.crowdstrike.com/falcon-host/index.html (last accessed June 16, 2025)
2017	<i>YouTube</i> , “CrowdStrike Falcon Use Case: True Endpoint Visibility,” Oct. 13, 2015, https://www.youtube.com/watch?v=pHxb6EyjhPw (last accessed June 20, 2025)
2018	LinkedIn, <i>Dmitri Alperovitch – Experience</i> , https://www.linkedin.com/in/dmitrialperovitch/details/experience/ (last accessed June 18, 2025)

Exhibit	Description
2019	Wayback Machine archive of <i>CrowdStrike</i> , “Our Team,” archived February 26, 2014, https://web.archive.org/web/20140226192409/http://www.crowdstrike.com/our-team/index.html (last accessed June 18, 2025)
2020	Wayback Machine archive of <i>CrowdStrike</i> , “CrowdStrike Recognized on CRN’s Security 100 List,” archived April 13, 2016, https://web.archive.org/web/20160413184238/http://www.crowdstrike.com/crowdstrike-recognized-on-crns-security-100-list/ (last accessed June 20, 2025)
2021	Wayback Machine archive of <i>CrowdStrike</i> , “CrowdStrike Named 2015 Technology Pioneer by World Economic Forum,” archived April 13, 2016, https://web.archive.org/web/20160413185023/http://www.crowdstrike.com/crowdstrike-named-2015-technology-pioneer-by-world-economic-forum/ (last accessed June 20, 2025)
2022	Wayback Machine archive of <i>CrowdStrike</i> , “Resources – Case Studies,” archived March 31, 2016, https://web.archive.org/web/20160331144104/http://www.crowdstrike.com/resources#case-studies (last accessed June 20, 2025)
2023	Wayback Machine archive of <i>CrowdStrike</i> , “CrowdStrike Closes \$100 Million Financing Round Led by Google Capital,” archived March 29, 2016, https://web.archive.org/web/20160329225128/http://www.crowdstrike.com/crowdstrike-closes-100-million-financing-round-led-by-google-capital (last accessed June 20, 2025)

Exhibit	Description
2024	Wayback Machine archive of <i>CrowdStrike</i> , “Google Capital Bets Big on CrowdStrike to Accelerate Hyper-growth,” archived Dec. 20, 2015, https://web.archive.org/web/20151220114826/http://www.crowdstrike.com/blog/google-capital-bets-big-on-crowdstrike (last accessed June 20, 2025)
2025	Plaintiff's First Set of Requests for Production to CrowdStrike (Nos. 1-59), in <i>GoSecure, Inc. v. CrowdStrike, Inc.</i> , Case No. 1:24-cv-00526-DII (W.D. Tex., Aug. 16, 2024)
2026	(Proposed) Default Protective Order
2027	Wayback Machine archive of <i>CrowdStrike</i> , “CrowdStrike™ Named 2014 SINET 16 Innovator,” archived Feb. 22, 2017, https://web.archive.org/web/20170222022251/https://www.crowdstrike.com/resources/crowdstrike-named-2014-sinet-16-innovator/ (last accessed June 20, 2025)
2028	<i>CrowdStrike, Inc. v. NSS Labs, Inc.</i> , No. 17-cv-146 (D. Del. Jan. 18, 2018), Dkt. 35 (redacted version of Second Amended Complaint)
2029	CrowdStrike Job Listing on Accel, https://jobs.accel.com/companies/crowdstrike/jobs/36416955-sr-analyst-sales-analytics-remote (last accessed October 9, 2025)
2030	CrowdStrike Falcon© Go, https://www.crowdstrike.com/en-us/pricing/falcon-go/ (last accessed October 9, 2025)
2031	Declaration of Angelos Stavrou
2032	<i>Curriculum vitae</i> of Angelos Stavrou
2033	Markus Jakobsson Deposition Transcript taken on November 11, 2025

Exhibit	Description
2034	Anne Arness, “What is EDR ? Endpoint Detection and Response (EDR)?” January 7, 2025, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (last accessed November 26, 2025)
2035	CrowdStrike Holding, Inc. Initial Public Offering SEC Filing
2036	US 8,656,493 (Capalik 493)
2037	US 2008/0320594 (Jiang)
2038	US 2012/0331553 (Aziz)
2039	US 2006/0136720 (Armstrong)
2040	US 7,356,845 (Jakobsson)
2041	Bart Lenaerts-Bergmans, “What is a Backdoor Attack?” July 17, 2023, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/backdoor-attack/ (last accessed November 26, 2025)
2042	Arfan Sharif, “What is CVE? Common Vulnerabilities & Exposures,” December 7, 2022, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/common-vulnerabilities-and-exposures-cve/ (last accessed November 26, 2025)
2043	Bart Lenaerts-Bergmans, “What is Hacktivism?” July 7, 2022, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/hacktivism/ (last accessed November 26, 2025)

Exhibit	Description
2044	Thuy Nguyen, "What are Tailgating and Piggybacking Attacks?" June 25, 2025, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/tailgating-piggybacking-attack/ (last accessed November 26, 2025)
2045	Cybersecurity 101: The Fundamentals of Cybersecurity, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ (last accessed November 26, 2025)
2046	David Rojas and Mark Robinson, "Hiding in Plain Sight: Remediating "Hidden" Malware with Real Time Response," December 16, 2020, available at: https://www.crowdstrike.com/en-us/blog/how-to-remediate-hidden-malware-real-time-response/ (last accessed November 26, 2025)
2047	Kurt Baker, "Bootkit: Definition, Prevention, and Removal," January 4, 2023, available at: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/bootkits/ (last accessed November 26, 2025)
2048	M. Churchill, "Parsing Sysmon Events for IR Indicators," February 23, 2015, available at: https://www.crowdstrike.com/en-us/blog/sysmon-2/ (last accessed November 26, 2025)
2049	Microsoft Computer Dictionary, p. 105 (4 th ed. 1999)
2050	Heng Yin, Zhenkai Liang and Dawn Song, "HookFinder: Identifying and Understanding Malware Hooking Behaviors," October 17, 2007, CyLab, CMU
2051	Video: Introduction to CrowdStrike, available at: https://www.youtube.com/watch?v=n2LkiwbAYCI (Jan. 25, 2013) (last accessed December 11, 2025)

Exhibit	Description
2052	Stephen T. Jones, Andrea C. Arpaci-Dusseau, and Remzi H. Arpaci-Dusseau, "VMM-based Hidden Process Detection and Identification using Lycosid," <i>Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments</i> , 2008.
2053	Markus Jakobsson Deposition Transcript taken on April 15, 2026
2054-2099	RESERVED
2100	CounterTack Board of Directors Meeting Slides, Feb. 27, 2012 [PROTECTIVE ORDER MATERIAL]
2101	CounterTack Internal Meeting Invitation, Nov. 23, 2011 [PROTECTIVE ORDER MATERIAL]
2102	NeuralIQ internal email re: Jeremy Gould [PROTECTIVE ORDER MATERIAL]
2103	Alperovitch email re: Jeremy Gould [PROTECTIVE ORDER MATERIAL]
2104	Gould farewell email [PROTECTIVE ORDER MATERIAL]
2105	Alperovitch farewell email [PROTECTIVE ORDER MATERIAL]
2106	Minutes of the Feb. 27, 2012 Meeting of the Board of Directors of CounterTack Inc. [PROTECTIVE ORDER MATERIAL]

I. Introduction

CrowdStrike's Reply misuses the '872 patent to bridge the gaps between Capalik and the claims. Where CrowdStrike cannot find the claimed subject matter in Capalik, it borrows from the '872 patent itself and then asserts that because the '872 patent teaches it, Capalik must too. Yet the cited teachings of the '872 patent are nowhere to be found in Capalik.

If the claimed subject matter were truly disclosed in Capalik, CrowdStrike would not need to piece together arguments from bits of both the '872 patent and Capalik specifications. The Reply's continued reliance on the '872 patent in its obviousness analysis is improper, and the Board should reject it.

CrowdStrike has failed to meet its burden in this proceeding, and Patent Owner has shown that every challenged claim is patentable over the prior art.

II. Ground 1

A. Limitation 1[c]

The POR showed that the stored data structure is a key distinction between *Capalik* and the '872 patent. POR at 18. The Petition—and now the Reply—fails to identify where Capalik discloses the claimed “data structure that identifies, for each of a plurality of activities, the activity sources, activity targets, and associations.”

In its Reply, CrowdStrike moves the goalposts. CrowdStrike now uses the specification of the '872 patent itself—portions that are not in Capalik—to try to connect Capalik's "forensic data" with limitation 1[c]. There is no evidence that a POSITA would have understood Capalik's generic "forensic data" to teach these distinctive portions of the '872 patent. CrowdStrike's approach is improper and should be rejected.

Nevertheless, CrowdStrike is also wrong. CrowdStrike uses the '872 patent for gap-filling for both the assertion that (1) forensic data is the claimed data structure; and (2) forensic data identifies activity sources, targets, and associations. Reply at 4-9. Neither is true.

1. The '872 patent does not equate "forensic data" to the claimed "data structure"

Unable to find the claimed data structure in Capalik, CrowdStrike now *looks to the '872 patent* to connect the dots between the term "forensic data" and the claimed data structure. Specifically, CrowdStrike asserts that "the ['872] patent does not materially distinguish between forensic data and the claimed data structure." Reply at 6. That is false.

The '872 patent uses the term "forensic data" only twice. Both passages use the term as a generic term for data collected or generated during monitoring. *See* '872 patent, 7:14-18 ("[T]he introspection module examines the contents of

memory segments ... in an instrumented context that generates and retrieves forensic data (or fingerprint)."); 10:31-33 ("The raw attack information is then communicated to and stored on the database server 128 as forensic data 236 for later analysis."). Neither passage equates "forensic data" with the claimed data structure.

Separately, the '872 patent discusses data structures in relation to Figures 5A-5C. '872 patent, 3:40-46. Figure 5A is described as "a block diagram illustrating exemplary *data structures* of unauthorized activity data 502 and unauthorized activity entries 505." '872 patent, 12:45-48. The '872 patent goes into detail about this structure including various groupings and variables. *See* '872 patent, 12:45-13:64.

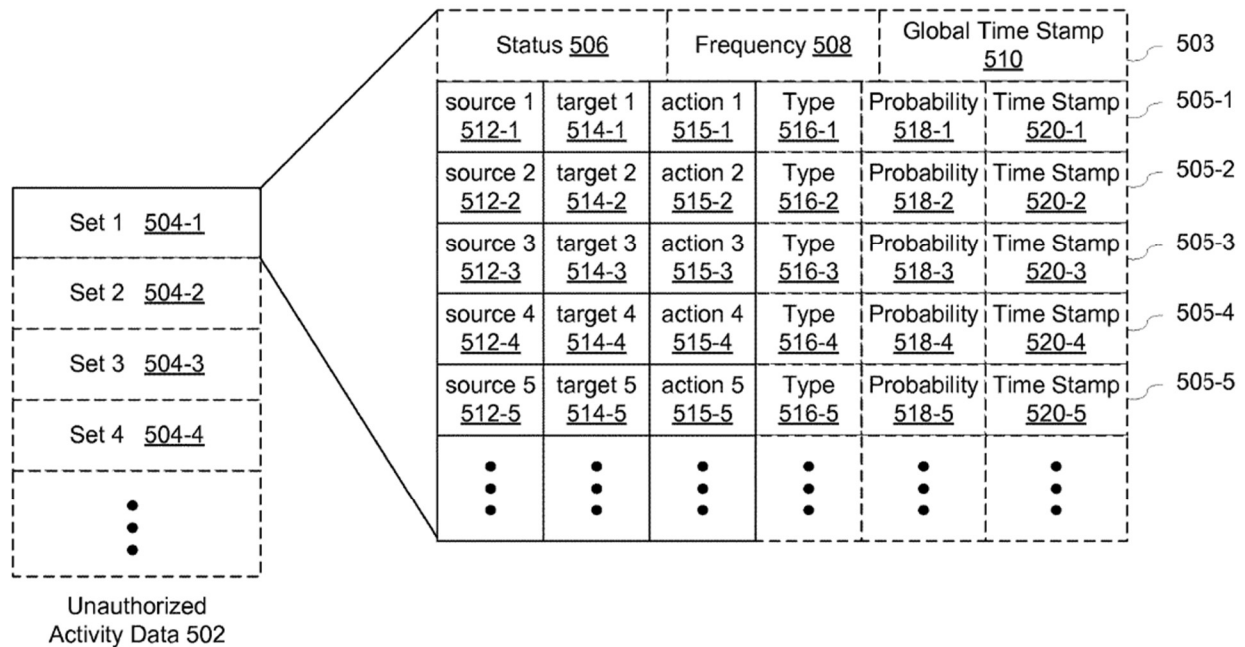
**Figure 5A**

Figure 5A and its associated description are *not in Capalik*. In fact, Capalik does not use the term “data structure” at all.

CrowdStrike does not even cite the '872 patent to support its assertion that there is no “material[]” distinction between forensic data and the data structure. Instead, CrowdStrike cites only Dr. Stavrou’s deposition testimony. Reply at 6. But that exact testimony refutes CrowdStrike’s baseless conflation of “forensic data” and the claimed data structure. Ex. 1034, 70:19-71:11. CrowdStrike asked Dr. Stavrou if “the forensic data produced by the introspection module [is] sufficient to teach [the claimed] data structure,” and he answered:

[T]he information you need to create the data structure might be present, but the formation, storage and identification of the specific

elements of data activity sources and activity target and associations have to be present and clearly delineated and stored in memory for a data structure to happen.

Id.; see also *id.* at 79:2-12 (“Q. Is the raw forensic data... sufficient to satisfy the claimed data structure? A. ...[L]ogs are not usually organized in the form of a data structure that clearly delineates activity sources, activity targets and associations for a variety of activities. And I didn’t see any mention of that in Capalik.”).

Thus, Dr. Stavrou’s testimony directly refutes CrowdStrike’s new assertion that there is no distinction between forensic data and the claimed data structure in the ’872 patent.

CrowdStrike also cites Figures 5B-5C *of the ’872 patent* as somehow disproving that “forensic data is converted to the claimed data structure before a fingerprint is generated”—again trying to collapse “forensic data” into the claimed data structure. Reply at 7. The opposite is true. These figures and their associated descriptions (none of which are in Capalik) do not use the term “forensic data” at all. The ’872 patent’s consistent use of “data structure” to describe these figures, but “forensic data” in more generic contexts, supports that mere forensic data is not sufficient to disclose a data structure.

Further, CrowdStrike misses the point by emphasizing that Figures 5B-5C are labeled as “fingerprint[s].” The ’872 patent does not need to show some

conversion from forensic data to a data structure in order for the term “data structure” to have a distinct meaning. Nevertheless, as noted above, Figure 5A is a “data structure” and is *not* described as a fingerprint, demonstrating that the data structures for fingerprints in Figures 5B-5C can be generated from a data structure rather than only from “forensic data.” ’872 patent, 12:45-48.

But again, CrowdStrike fails to explain the relevance of these assertions because *none of this is in Capalik*. At most, Capalik discloses unspecified “forensic data.” It does not disclose any data structure that identifies the source, target, and associations between source and target for each identified activity. The contrast is stark: the ’872 patent devotes multiple figures (3A-3C, 4A-4E, 5A-5C) and extensive specification text to describing the claimed data structure—Capalik has none.

Nor is there any inconsistency in GoSecure’s argument that CrowdStrike’s later-developed *graph* database practices the claims. *See* Reply at 7-8. A graph is a data structure, and CrowdStrike’s graph database stores a data structure. Capalik does not disclose any graph, node structure, or relational data structure. CrowdStrike’s comparison of its own “graph database” to Figure 3C *of the ’872 patent* underscores the absence of such disclosure in *Capalik*. Reply at 8. Capalik’s silence speaks volumes—it does not disclose this concept at all.

CrowdStrike handwaves that “Capalik teaches the same functionality, using nearly identical language”—but Capalik does *not* teach Figure 3C either visually or with text. Figure 3C depicts activity sources, targets, and associations organized in a graph structure that shows how process A, file X, file Y, and process B are related through specific associations. ’872 patent, Fig. 3C. None of that is in Capalik. *See* ’872 patent, 11:45-12:26.

2. The ’872 patent does not demonstrate that *Capalik’s* “forensic data” identifies activity sources, targets, and associations.

CrowdStrike is also unable to show that Capalik’s “forensic data” identifies activity sources, targets, and associations. Again, it turns to the ’872 patent to find that connection. Reply at 5-6. Again, that approach is improper.

CrowdStrike’s theory is based on an unsupported inference that monitoring activity sources, targets, and associations means Capalik’s “forensic data” identifies all of these activity sources, targets, and associations. Reply at 5 (CrowdStrike’s alleged “actual theory”). But CrowdStrike has nothing in Capalik to support that inference. Monitoring activity and storing “attack information” does not establish the claimed data structure that identifies activity sources, targets, and associations for multiple activities. In the Petition, CrowdStrike relied on the subsequent formation of a signature to try to show the content of “forensic data,” but GoSecure showed in its POR that CrowdStrike had failed to show that

Capalik's signature contained all three categories for each identified activity. *See* POR at 17-18. CrowdStrike does not dispute that assertion.

With nothing in Capalik to support its theory, CrowdStrike again looks to the '872 patent—this time Figures 3A-3C. Reply at 5. CrowdStrike then asserts that “Capalik teaches the very same functionality, using nearly identical language..., so its forensic data also identifies the claimed data fields.” Reply at 6. That is wrong, because *these figures are not in Capalik*.

Figures 3A-3C of the '872 patent do not support the assertion that Capalik's forensic data must also identify the claimed categories. CrowdStrike asserts that Dr. Stavrou “identified Figs. 3A-3C as ‘exemplars’ of the generated forensic data and confirmed that the data ‘shows the attacker[,] . . . shows the source[, and] shows the association and the target.’” Reply at 5 (citing Ex. 1034, 93:6-21). The record shows otherwise. When asked whether the '872 patent describes Figure 3 as “raw forensics data,” Dr. Stavrou unequivocally answered: “No, sir.” Ex. 1034, 149:10-12; *id.* at 149:17-23. Dr. Stavrou also testified that he “did not intend to equate raw forensic data in the '872 patent with a graph form or the structure that's shown in Figure 3A.” *Id.* at 150:6-10.

The POR showed that storage of mere “attack information” as “forensic data”—Capalik's actual disclosure—does not satisfy the claim. POR at 14-16.

CrowdStrike's reliance on the '872 patent to cure Capalik's deficiencies is improper.

B. Limitation 1(d)

The POR showed that Capalik does not disclose transmission of information to another computer system “for preventing future attacks” to the other computer systems. POR at 19-22. The POR further showed that CrowdStrike and its expert treated the term “computer system” as a ball of “dough” that could mean anything the reader wanted it to mean. POR at 36-37 (quoting Ex. 2033 57:7-60:10).

In Reply, CrowdStrike asserts that then-Acting Director Stewart somehow endorsed its construction *by not addressing it* when vacating institution based on discretionary denial. Reply at 10. Not so. There can be no “implicit[]” endorsement of CrowdStrike's improper construction where the Acting Director granted Director Review and vacated the institution decision on other grounds.

The POR also showed that CrowdStrike changed its mapping and proposed a new claim construction after the POPR was filed in this proceeding. POR at 23-24. In Reply, CrowdStrike asserts that the Petition made this mapping, yet it cannot find any such language in the Petition. *See* Reply 11 (citing only to its explanation that the information is sent to the IDS to prevent access to the protected network).

CrowdStrike also argues that it was allowed to “elaborate or clarify it theory” after the Petition was filed. Reply at 11 (citing *Apple Inc. v. Andrea Elecs.*

Corp., 949 F.3d 697, 706 (Fed. Cir. 2020)). But this was no elaboration, it was a brand new claim construction and a brand new mapping based on that construction. *See* POR at 23. The Board should not permit a petitioner to make new mappings based on new constructions after the POPR.

On the merits, CrowdStrike's Reply repeatedly—and incorrectly—makes arguments that simply assume its construction is correct. For example, CrowdStrike asserts that the '872 patent uses the term “computer system” to refer to protected network 504. Reply at 11-13. CrowdStrike asserts that in the '872 patent, “a first computer system—decoy computer network comprising decoy network device—communicates via a network connection with a computer system—protected computer network comprising an IDS/IPS system and protected network devices.” Reply at 11. But the '872 patent *never* calls a protected network—or any network—a computer system. CrowdStrike does not even cite any portion of the '872 patent to support this assertion, it merely annotates figures that do not even use the term “computer system”. *See* Reply at 12 (annotating '872 patent, Fig. 1). CrowdStrike simply assumes this to be true and then repeats it several times. *See* Reply at 13 (“the '872 Patent ... embraces groups of devices (e.g., protected network 504) as computer systems.”), 14 (““computer system’ is used broadly such that both disclosed embodiments are captured” by CrowdStrike's construction).

Not once does the '872 patent use “computer system” to refer to a network. And CrowdStrike has no rebuttal to the plethora of evidence supporting that the ordinary and customary use of computer system precludes it from being a network. CrowdStrike merely asserts the Board should ignore it because of that single use of “distributed computer system” to refer to a system that CrowdStrike does not dispute is *not* an embodiment of claim 1. Reply at 15.

C. Claim 2

CrowdStrike has the burden to show that Capalik discloses “monitoring all activity on the *first computer system*” as recited in claim 2. Capalik's VM is not the alleged “first computer system.”¹ Pet. 15. Rather, the Petition identifies “decoy computer 502” as the “first computer system.” Pet. 15.

For this claim, the Petition simply asserts that Capalik monitors *some* activity on *a subset of* the first computer system. *See* POR 43-44 (citing Pet. 34). CrowdStrike now attempts to rewrite the claim to fit its Petition, i.e., that the claim requires monitoring only a subset of activity. Reply 16-20. That is wrong.

¹ Nor could it be, because the alleged storing step is not “in the memory” of the VM. *See* cl. 1 (“wherein the first computer system comprises... memory” and “storing in the memory...”).

Capalik does not satisfy the plain claim language. The POR showed that Capalik does not monitor all activity on the alleged first computer system, which the Petition mapped to a “decoy computer 502” in Fig. 2. POR at 43-54. Namely, the decoy computer 502 included significant unmonitored activity outside of the monitored VM (POR at 51-53) as well as unmonitored activity before an attack received at a socket (POR at 46-51).

In Reply CrowdStrike does not dispute that Capalik's monitoring is limited as identified in the POR. Instead, CrowdStrike now attempts to rewrite claim such that monitoring can be performed (1) only within a VM and (2) only “after an attack is received.” Reply at 19-20. That is not the plain language of claim 2.

Capalik does not monitor all activity on the “decoy computer 502”

First, CrowdStrike's attempt to read a VM into claim 2 is improper. *See* Reply at 19-20 (“PO is wrong that the claim language requires monitoring activity outside the VM.”). Claim 2 does not recite a virtual machine. Its language is plain and clear: “monitoring all activity on the first computer system.” Nor does the specification of the '872 patent support reading a VM into claim 2, contrary to CrowdStrike's mischaracterizations. *See* '872 patent, 11:18-21 (“[A]nalogous methods can be used to represent and analyze unauthorized activities on ***non-virtualized computer systems***.”).

Decoy computer 502—undisputedly—contains many unmonitored activities including an entire unmonitored operating system. CrowdStrike misrepresents GoSecure's argument as finding "fault in Capalik's failure to monitor its own monitoring." Reply at 16. Not so. Decoy computer 502 contains a "processing module 508" that is neither the monitor nor something that is monitored. *See* Pet. 23 (mapping Capalik's introspection module 538 to the monitor), Capalik Fig. 5. The processing module 508 is a separate entity within decoy computer 502 "for obtaining, analyzing, and responding to exploits." Capalik [0038]. It has its own operating system. Capalik [0051].

CrowdStrike's approach here is almost identical to its approach that the Board rejected in parallel IPR Petitions. *See CrowdStrike, Inc. v. GoSecure, Inc.*, IPR2025-00067, Paper 13 at 9 (PTAB May 6, 2025). There, the Board rejected CrowdStrike's attempt to rewrite the plain language of a claim of the '872 patent's parent, based on comparison of specifications with Capalik. *See id.* at 8-9. The Board should reject the same argument here.

To the extent CrowdStrike implies that it would be absurd to monitor this entire operating system within the alleged "first computer system," even with the benefit of hindsight, that speaks to the non-obviousness of claim 2 and the failure of CrowdStrike to carry its burden in this proceeding.

Capalik does not even monitor all activity on the VM

Capalik does not even disclose monitoring all activity on the VM. Consequently, CrowdStrike attempts to limit the claim to monitoring activity “*after*” an attack. Reply at 19.

CrowdStrike does not dispute that Capalik does not monitor any activity before an attack occurs. Instead, CrowdStrike asserts that in Capalik, “there is nothing to detect unless the VM is being attacked.” Reply at 17. But that is not how computers work. Capalik uses conventional operating systems to provide the illusion of a vulnerable computer. Capalik at [0008] (“decoy network appliance... runs fully functional operating systems”), [0023] (discussing use of off-the-shelf Microsoft Windows and LINUX operating systems). As confirmed by Dr. Jakobsson, such conventional operating systems run background tasks even without any interaction. Ex. 2053 at 126:7-127:18 (describing the various responsibilities of operating systems and “background tasks” that run without user interaction).

But CrowdStrike's argument goes to the key assumption of Capalik: that there is nothing *suspicious* happening at the node until an attack is received. Reply at 17. That assumption distinguishes claim 2 from Capalik. And CrowdStrike's attempt to equate the *specifications* of Capalik and the '872 patent is both

irrelevant and improper for the reasons discussed above. *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1373-75 (Fed. Cir. 2004).

III. Ground 2 – Capalik / Goel

The POR showed that a POSITA would not have been motivated to combine Capalik and Goel because Goel's monitoring is detectable by attackers, rendering Capalik's decoy system inoperable for its intended purpose. POR at 55-59. Specifically, Goel's monitoring is detectable both because (1) it noticeably slows down the system, and (2) it uses detectable operating system "hooks." POR at 57. The POR showed that Goel is not a decoy system and has no concern about detectability, and therefore its monitoring is detectable. POR at 56-57. Indeed, the Petition acknowledged an "increase in processing power required to modify Capalik per Goel's teachings." Pet. at 44-45.

In Reply, CrowdStrike does not dispute the detectability of the combined system based on slowing down the system. CrowdStrike even acknowledges a "tradeoff between effectiveness and efficiency." Reply at 20-21 (citing Pet. at 43-46). Goel's monitoring is indisputably detectable based on the slowdown, and that alone is fatal to CrowdStrike's combination.²

² CrowdStrike uses a footnote to address detectability, asserting that the '872 patent itself "slows the system enough to raise an attacker's suspicion." Reply at

Instead, CrowdStrike focuses on the second way that Goel's monitoring is detectable, asserting that the combination would not include Goel's detectable "hooks." Reply at 21. This is pure revisionism motivated by CrowdStrike's desire to fix its Petition. The Petition explained that a POSITA would have had a reasonable expectation of success because Goel teaches "that its system implementation can be achieved by adding lines of code." Pet. 46. And for that code, the Petition specifically calls out Goel's "auditing module code" that is "derived from the SNARE project." Pet. 46 (citing Goel, 4-5). The "auditing module code" comprises the exact hooks GoSecure showed are detectable: hooks that "hijack[] the system call table and add[] stub code around several system calls to capture the system call, its timing, its parameters, its return value and the PID of the process making the call." Goel at 4, §5.1. In other words, the "lines of code" that the Petition combines into Capalik *are the hooks*. Indeed, this is "Goel's known technique" that the Petition proposes to incorporate into Capalik. Pet. 44.

21, n.6 (citing '872 patent, 7:43-53). This is false. The passage cited by CrowdStrike describes that an attacker could identify that the computer is running on a virtual machine due to its performance, but explicitly states—in the very next sentence that CrowdStrike omits—that the attacker would not be able to detect the introspection module. '872 patent, 7:43-50.

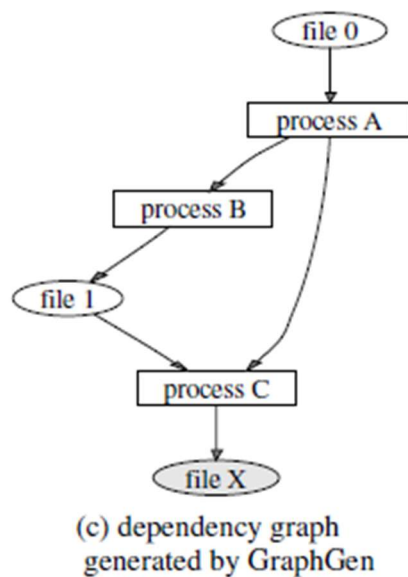
The Petition provides no other explanation as to how a POSITA could have implemented Goel's monitoring in Capalik without such hooks. CrowdStrike's post-hoc attempt to walk away from them is improper.

Finally, *In re Keller* is inapposite. Reply at 21-22. GoSecure is not arguing about bodily incorporation, or that Goel can't be incorporated into Capalik. The argument is simple: the combination results in detectability, and a POSITA would not have done it. For that reason, Ground 2 fails.

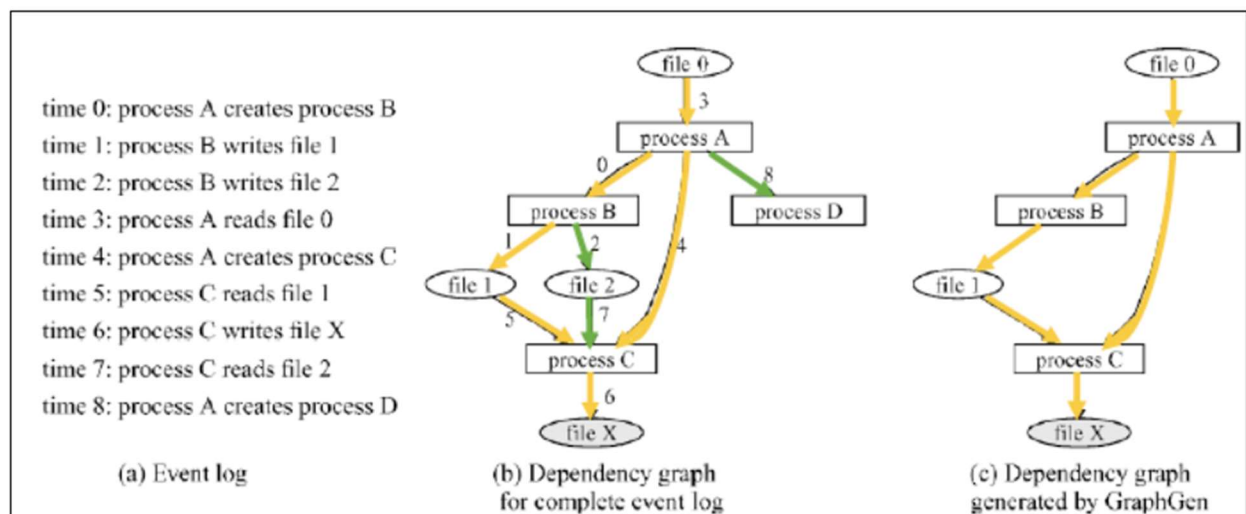
IV. Ground 3

A. Claim 8.

The POR showed that King's dependency graph in Fig. 3.2(c), below, does not "visually distinguish[] at least a subset of the associations." POR at 59-61. According to CrowdStrike's mapping, the lines connecting files and processes constitute associations. And as shown below, none of these lines are "visually distinguish[ed]" when graphically displayed. POR at 59-61.

**King, Fig. 3.2(c)**

In Reply, CrowdStrike rehashes the same failed argument from the Petition, trying to create the illusion of a visual distinction by adding color on top of the arrows and comparing Fig. 3.2(c) to Fig. 3.2(b). Reply at 22-23.

**Reply at 22 (annotating King, Fig. 3.2)**

Specifically, CrowdStrike asserts that “[w]hen King *displays the full Fig. 3.2(b)* dependency graph, it displays at least a subset of the stored activities, but does not distinguish between malignant and benign associations.” Reply at 23. But, as the POR explained, Fig. 3.2(b) is *never displayed*, and CrowdStrike does not rebut this. See POR at 60 (“King does not contemplate actually displaying Fig. 3.2(b).”).

CrowdStrike is unable to explain how King’s Fig. 3.2(c)—the only thing that King actually displays—both qualifies as displaying a subset of activities (claim 7) and “visually distinguishing” a subset of the associations (claim 8). Instead, CrowdStrike asserts that the claims recite “different subsets.” Reply at 22-23. But that distinction is not material. The associations are part of the activity, as recited in claim 1 (“each of the activities includes... an association”). Thus, by “graphically displaying” a subset of the activities, claim 7 already requires graphically displaying a subset of the associations. Claim 8 requires more.

But King does not do more than display a subset of events (the alleged “activities”). See King at 26 (“GraphGen considers the *event* at time 8. This *event* does not affect any object in the current graph (i.e. file X), *so we ignore it.*”). In particular, it does not visually distinguish any associations. Thus, CrowdStrike has not shown that claim 8 is obvious.

B. Claim 16.

CrowdStrike attempts to reframe its Petition and improperly incorporate its expert's testimony by reference. In Reply, CrowdStrike states that "[t]he Petition explained that King's filtered dependency graph Fig 3.2(c) is created *only after* the system has determined a complete status." Reply at 23.

CrowdStrike's Reply argument is improper because it was not in the Petition. The Petition asserted that "King's Fig. 3.2(c) illustrates a complete activity status for an attack." Pet. at 63. That assertion says nothing about creating Fig. 3.2(c) "only after" determination of a complete status.

To the extent CrowdStrike 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. 37 C.F.R. §42.6(a)(3).

Nevertheless, even if the Board were to consider paragraph 231 and CrowdStrike's new argument, it still fails to show that King discloses the features of claim 16. King does not disclose creating filtered dependency graph Fig 3.2(c) "*only after* the system has determined a complete status." Reply at 23. 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. *See* POR at 62. CrowdStrike's Reply does not address this argument.

This argument stands un rebutted, and CrowdStrike has not met its burden for claim 16. CrowdStrike never identifies any step in King that determines whether stored activities have a “complete” or “incomplete” status.

C. Claim 19.

CrowdStrike admits that “the Petition did not explicitly identify where precisely King’s ‘type’ would be organized as a distinct data field in Capalik’s forensic data structure.” Reply at 25. That failure alone is dispositive. But the Petition’s failure for claim 19 is even more severe than CrowdStrike acknowledges. The claim requires that “the association includes a type that represents whether or not the activity source has modified the activity target to perform the unauthorized activities.” This “type” must be part of the association that is stored in the data structure required by claim 1. *See* ’872 patent, Fig. 5A (depicting “Type” field 516 as part of each activity entry in the stored data structure). As shown in the POR, the Petition did not even attempt to address how the combination would disclose storing a data structure that identifies the claimed association “type.” POR at 65-66. CrowdStrike’s Reply concedes this failure—and then tries to excuse it by arguing that “the claims do not mandate that the claimed data structure be maintained in any particular format.” Reply at 25. The plain language of the claim says it does—the data structure must identify the claimed “type” for each activity. CrowdStrike has no answer because there is none.

CrowdStrike cannot meet its burden by failing to address a requirement of the claims and then excusing that failure by asserting—without support—that the requirement does not matter.

V. Ground 4 (Claim 13)

CrowdStrike argues that the POR's arguments are "unsupported attorney argument" and "[w]ithout expert testimony." Reply at 26. But Dr. Stavrou provided such testimony supporting the POR's arguments. Ex. 2031, ¶¶95-96.

CrowdStrike again attempts to read the specification of the '872 patent into the prior art. CrowdStrike cites to the '872 patent's passage describing "data execution prevention (DEP) mechanisms" which "can generate an exception when there is an *attempt* to execute an instruction that is set as non-executable." '872 patent, 16:13-20; Reply at 25. But that's not what Pike teaches. Pike does not use the term "data execution prevention" or "DEP". Further, 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*." Pike, 8:65-67; Pet. at 67. CrowdStrike's attempt to read the '872 patent into Pike is legal and technical error.

VI. Objective indicia

Refusing to put its money where its mouth is, CrowdStrike faults the POR for providing "insufficient" evidence when CrowdStrike fought tooth-and-nail in

jurisdictions across the country to prevent any discovery into records of its copying. But direct evidence is not required to show copying, and none is needed here. CrowdStrike's public literature demonstrates that its products—created by former GoSecure insiders—practiced claims 1 and 2 of the '872 patent from the onset, and received widespread commercial success and industry praise specifically for the claimed innovations.

VII. Conclusion

The Board should find all challenged claims non-obvious.

Respectfully submitted,

Dated: April 23, 2026

By: /s/ Steven W. Peters

Steven W. Peters (Reg. No. 73,193)
speters@cgsh.com
CLEARY, GOTTlieb, STEEN & HAMILTON LLP
2112 Pennsylvania Ave., NW
Washington, D.C. 20036
Telephone: 202.974.1813

*Counsel for Patent Owner
GoSecure, Inc.*

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

I hereby certify that this Patent Owner's Sur-Reply complies with the word count limitation of 37 C.F.R. § 42.24(b)(1) because the Patent Owner's Sur-Reply contains 4,307 words using Microsoft Word's counting feature, excluding the cover page, signature block, and the parts of the Patent Owner's Sur-Reply exempted by 37 C.F.R. § 42.24(b)(1).

By: /s/ Steven W. Peters

Steven W. Peters (Reg. No. 73,193)
speters@cgsh.com
CLEARY, GOTTlieb, STEEN & HAMILTON LLP
2112 Pennsylvania Ave., NW
Washington, D.C. 20036
Telephone: 202.974.1813

*Counsel for Patent Owner
GoSecure, Inc.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 23rd day of April, 2026, a true and correct copy of the foregoing **Patent Owner's Sur-Reply and Exhibit 2053** were served by electronic mail on Petitioner's lead and backup counsel at the following email addresses:

Paul R. Hart, (Reg. No. 59,646)
Paul.Hart@eriseip.com
PTAB@eriseip.com
ERISE IP, P.A.
717 17th St., Suite 1400
Denver, Colorado 80202
Telephone: 913.777.5600
Fax: 913.777.5601

Adam P. Seitz (Reg. No. 52,206)
Adam.Seitz@eriseip.com
ERISE IP, P.A.
7015 College Blvd., Suite 700
Overland Park, Kansas 66211
Telephone: 913.777.5600
Fax: 913.777.5601

By: /s/ Steven W. Peters

Steven W. Peters (Reg. No. 73,193)
speters@cgsh.com
CLEARY, GOTTlieb, STEEN & HAMILTON LLP
2112 Pennsylvania Ave., NW
Washington, D.C. 20036
Telephone: 202.974.1813

*Counsel for Patent Owner
GoSecure, Inc.*