

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner

v.

GOSECURE, INC.,
Patent Owner

Case Nos. IPR2025-00070
U.S. Patent No. 9,954,872

PETITIONER'S REQUEST FOR REHEARING

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	LEGAL STANDARD.....	2
III.	THE BOARD’S ANALYSIS OF “ALL ACTIVITY” MISAPPREHENDED THE INTRINSIC RECORD	3
A.	Summary of the Parties’ Positions.....	3
B.	The Board Erred by Relying on Unpresented Arguments and Evidence.....	6
1.	Claim Differentiation Does Not Support the Board’s Construction.....	7
2.	The Specification Only Discloses Monitoring Attack Activities.....	9
C.	The Board Misunderstood Dr. Jakobsson’s Testimony	11
IV.	CLAIM 8 – THE BOARD DID NOT ADDRESS THE DISPUTE PRESENTED BY THE PARTIES	13
V.	CONCLUSION.....	15

I. INTRODUCTION

The Final Written Decision (“FWD”) canceled Claims 1, 3-7, and 9-21 of the ’872 Patent but declined to cancel Claims 2 and 8. FWD, (Paper 62), 69. Petitioner respectfully requests rehearing of the Board’s findings on Claims 2 and 8.

First, the Board’s decision on Claim 2 relied on a claim interpretation that is unsupported by the intrinsic record. Namely, the Board concluded that the monitored “all activity” of Claim 2 is not limited to attack activity, concluding that the specification supports such an interpretation by describing a system that monitors non-attack activity. FWD, 21-22 (“[C]ertain 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.”).¹ This analysis conflates the process of monitoring attack activities with the separate step of classifying attack activities as malignant, benign, etc. That monitored activities may be classified as benign does not mean they were not part of an attack. Indeed, not even PO advanced that reading of the specification. Instead, Patent Owner (“PO”) expressly argued at the hearing that Claim 2 needs no intrinsic support. Transcript (Paper 61), 76:25-77:6 (“*[I]t doesn't matter what the embodiments say or don't say*. Ultimately, the claim language is what counts.”). The

¹ All emphases added unless indicated otherwise.

Board correctly declined to adopt PO's position, but it erred by finding a critical teaching in the specification that is undisputedly not there. Because the Board's analysis turns on this misapprehension, rehearing is merited.

Second, the Board's decision on Claim 8 overlooked the arguments presented by the Parties regarding the meaning of "visually distinguishing" a subset of associations. Petitioner argued that King's process of filtering benign associations from an attack and displaying only the malignant associations satisfies both Claim 7's "displaying at least a *subset of* the stored *activities*" and Claim 8's "visually distinguishing at least a *subset of* the *associations*." Petition (Paper 1), 48-56. PO's sole substantive argument turned on claim differentiation. PO's Response ("POR") (Paper 47), 60. Petitioner's Reply explained that PO's claim differentiation argument fails because it ignores that each claim uses different language to describe what must be displayed. Reply (Paper 50), 22-23. The FWD did not address, let alone resolve, this sole dispute between the Parties. Accordingly, rehearing is merited.

II. LEGAL STANDARD

"A party dissatisfied with a decision may file a single request for rehearing" that "specifically identif[ies] all matters the party believes the Board misapprehended or overlooked, and the place where each matter was previously addressed in a motion, an opposition, a reply, or a sur-reply." 37 C.F.R. § 42.71(d).

III. THE BOARD’S ANALYSIS OF “ALL ACTIVITY” MISAPPREHENDED THE INTRINSIC RECORD

A. Summary of the Parties’ Positions

Claim 1 recites a “method of *identifying unauthorized activities* on a first computer system[.]” comprising “*monitoring activity* on the first computer” and “*transmitting . . . information identifying one or more of the activit[ies] . . . for preventing future attacks[.]*” Ex. 1001, Claim 1. Claim 2 further requires “monitoring *all activity* on the first computer system.” *Id.* at Claim 2. The Petition explained that both Capalik and the ’872 Patent utilize virtual machines (“VM”) to incentivize attacks and then monitor those attacks as they run in the VMs. Petition (Paper 1), 16-22 (for Claim [1(a)]’s monitoring limitation, showing the ’872 Patent and Capalik both monitor attacks as they run in VMs). For Claim 2, the Petition explained that *Capalik teaches monitoring all attack activity* in a VM “whenever” an attack gains access “through a VM network port[.]” *Id.* at 34 (incorporating Claim [1(a)] analysis and concluding that Capalik monitors all attack activity in a VM).

As confirmed at the hearing, Petitioner interpreted the claimed “activity” as attack activity, consistently with all embodiments, and advanced a theory that Claim 2 is satisfied by monitoring all attack activities. Transcript, 27:14-28:5 (“*Capalik monitors all attack activity* in its [VM] running on the decoy device. *That is what claim 2 is talking about. . . . [I]n 100 percent of the embodiments, the monitoring*

in the '872 Patent is limited to monitoring attacks[.]”), 28:14-21 (“[I]t really comes back to *what is the activity that this claim requires to be monitored*. And *it's very clear in the context of the claim and certainly in the context of the '872 specification: it is attack activity[.]*”), 28:25-29:2 (same).

PO advanced two arguments against Petitioner’s Claim 2 theory. First, PO manufactured an alleged distinction between Capalik and the ’872 Patent, arguing that (1) Capalik monitors activities in the virtual machine only after an attack is detected at a VM socket and (2) the ’872 Patent monitors activities in a VM independent of detecting the attack’s arrival at the VM socket. POR, 44-51. In support of (2), PO and its expert pointed to Figs. 4A-4D in the ’872 Patent, which collectively depict the process of detecting ***attack activity*** occurring on the VM and tracing the attack back in time to identify the specific socket the attack accessed. *Id.* PO’s interpretation of the ’872 Patent conflates the separate processes of (1) monitoring an attack and (2) analyzing activities within a monitored attack. In its Reply, Petitioner explained that there is ***no distinction*** between the activities monitored in Capalik and the ’872 Patent. Reply, 16 (“Both describe decoy systems running VMs that are intentionally left susceptible to attacks, so attacks to the VMs can be monitored.”), 17 (“Critically, in both systems, ***there is nothing to detect unless the VM is being attacked***. Ex. 1035, ¶¶4-10. The decoy device exists to be

attacked, and *until it has been attacked, there is no attack activity to monitor. Id.* Neither Capalik nor the '872 Patent describe monitoring activities outside a VM. Ex. 1035, ¶¶4-7"). Petitioner explained that, for PO's example, Figs. 4A-4D, the only reason these VM attack activities can be traced back to the attack's arrival is because all attack activities had been monitored. *Id.* at 17-19. That is, there is no monitoring prior to, or independent of, an attack. The '872 Patent, like Capalik, exclusively describes monitoring attack activities.

PO's second argument took aim at Petitioner's mapping of Capalik's decoy device as the "first computer system," insisting Petitioner was required to show Capalik monitored attack and non-attack activities both in and outside the VM. POR, 51-53. In its Reply, Petitioner explained PO's argument "is *inconsistent with all disclosed embodiments* and should be rejected." Reply, 19-20. PO's Sur-Reply focused entirely on this second argument, reiterating that, to prevail, Petitioner was required to show that Capalik monitors activity of every type in Capalik's entire decoy device. Sur-Reply (Paper 54), 11-15. Tellingly, at no point did PO identify a description in the '872 Patent of monitoring activities that are not part of an attack. And, at the hearing, PO effectively confirmed the point by expressly arguing that Claim 2 needs no intrinsic support. Transcript, 76:25-77:6 ("*[I]t doesn't matter what the embodiments say or don't say.*").

The Board’s decision turned on its conclusion that Claim 2’s “all activity” is *not* limited to “monitoring all attack activity” and instead requires monitoring both attack and non-attack activity. FWD, 22. In reaching this conclusion, the Board relied on two rationales that were never presented by either party. First, it introduced a claim differentiation analysis that neither party addressed in its papers. FWD, 20. Second, the Board concluded that the specification teaches monitoring non-attack activities—a position that PO never advanced and that misapprehends the intrinsic record. FWD, 21-22. The Board also misapprehended the testimony of Petitioner’s expert, Dr. Jakobsson, which is entirely consistent and supportive of interpreting Claim 2 such that only attack activities are monitored.

B. The Board Erred by Relying on Unpresented Arguments and Evidence

“[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.” *In re IPR Licensing, Inc.*, 942 F.3d 1363, 1368-69 (Fed. Cir. 2019) (citing *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016)). Meriting rehearing, the Board premised its claim construction finding on two arguments that were not advanced by the Parties and are not supported by the record.

1. *Claim Differentiation Does Not Support the Board's Construction*

The Board first erred by relying on claim differentiation between Claims 1 and 2 to determine “all activity” is broader than all attack activity. PO never advanced that argument, depriving Petitioner a meaningful opportunity to respond to it. Indeed, the entire record relevant to claim differentiation is a single exchange between the Board and Petitioner’s counsel at the oral hearing. *See* Transcript, 73:24-75:3. That exchange establishes that Claim 2 has a distinct meaning from Claim 1 under Petitioner’s construction. When asked what Claim 2 adds over Claim 1, Petitioner’s counsel directed the Board to the passage in the ’872 Patent describing two embodiments: one in which the introspection module monitors all attack activities and a second in which it monitors a subset based on monitoring priorities. Transcript, 73:24-75:3. Counsel explained that in both embodiments “everything that is being monitored is attack activity” and that “[b]oth those embodiments are captured by claim 1; only the monitoring all activity is captured by claim 2.” Transcript, 74:14-15; 74:20-21.

As Petitioner explained at the hearing, the ’872 Patent specification supports interpreting Claims 1 and 2 as monitoring only attack activity. The specification states that, in a first embodiment, “the introspection module monitors all activity (e.g., system calls, library calls, kernel calls, etc.) on virtualized decoy operating

systems 112.” Ex. 1001, 10:8-10. The specification clarifies that the reference to “all activity” refers to “all unauthorized activities,” when it contrasts a second embodiment that monitors activity “based on a monitoring priority (e.g., key system calls and kernel calls)” that “*may be set based on the type of unauthorized activities.*” *Id.* at 10:10-16. This passage confirms that the activities monitored are unauthorized (i.e., attack) activities—either all unauthorized activities or a specified subset of unauthorized activities. This is further confirmed by a related discussion that explains the introspection module monitors and captures information “[w]hen an attacker connects to a network port and begins interacting with a virtualized decoy operating system[.]” *Id.* at 9:67-10:7. Petitioner’s construction aligns with these embodiments while preserving meaningful differentiation between the claims. Claim 1 captures systems that monitor all attack activities, as in the first embodiment, and those that monitor only attack activities that exceed a priority level, as in the second embodiment. In contrast, Claim 2 captures only the first embodiment, requiring that all attack activities are monitored.

Had PO advanced claim differentiation as a basis to support its broad interpretation of “all activities,” Petitioner could have briefed these disclosures and explained why its construction preserves the distinction between Claims 1 and 2. PO did not, and the Board did not credit Petitioner’s response to its claim differentiation

theory posed for the first time at the hearing. Accordingly, rehearing is merited on this issue.

2. *The Specification Only Discloses Monitoring Attack Activities*

The Board also supported its construction by claiming that “*certain portions of the Specification indicate 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.” FWD, 21-22. PO correctly declined to rely on this passage in support of the position that “all activity” captures non-attack activity, as it does not support the Board’s conclusion that benign activities are non-attack activities. *See* POR, 43-54; Sur-Reply, 11-15; Transcript, 57:25-60:18. Instead, PO’s entire argument rested on the claim language itself, insisting “[t]he claim does not say monitoring all attacker activity or monitoring all malicious activity. It says monitoring all activity.” Transcript, 60:15-17. Because PO never relied on this passage to establish that the system monitors non-attack activity, Petitioner naturally did not explain why it does not.

In context, the passage cited by the Board does not support the Board’s conclusion that benign activities are non-attack activities. Characterizing individual attack activities as malignant or benign is a step that is applied to stored attack activities. The patent refers to this classification as the “type of association” for

individual *unauthorized (i.e., attack) activities* wherein a malignant activity has modified its target to perform unauthorized actions, and a benign activity has not. Ex. 1001, 13:16-50 (“Each set 504 in the *unauthorized activity data* 502 in FIG. 5A also *includes* one or more unauthorized activity entries” that include “one or more of . . . [a]n (optional) association type 516, which . . . may be . . . *malignant*, which represents that *the activity source 512 has modified the activity target 514 to perform unauthorized activities* [or] *benign*, which represents that *the activity source . . . has not modified the activity target 514 to perform unauthorized activities* (e.g., the instruction A reads the file X, but does not modify the file X)[.]”). Accordingly, that an individual activity has been classified as benign does not mean that it was not part of an attack. Rather, it simply means that this particular attack activity was deemed safe. To that end, the patent teaches that fingerprints used to protect other computer systems from damaging attacks can convey only the portions of an attack classified as malignant. *Id.* at 14:17-20. The Board’s cited passage merely describes distinguishing among types of attack activities. It does not suggest that the system monitors activity that is not part of an attack.

Every other passage of the ’872 Patent discussing monitoring “all activity” reinforces that the system only monitors unauthorized (i.e., attack) activity. For example, the specification states that in some embodiments “all activity on the

[VM]” is monitored because “*all activity on the [VM] is assumed [] to be unauthorized[.]*” Ex. 1001, 15:17-23, 15:10-13 (in some embodiments, “*all incoming data stream on the virtual machine is unauthorized*”), Fig. 6A. In these disclosures, as with every embodiment, the patent describes monitoring exclusively unauthorized (i.e., attack) activities.

Thus, the passage on which the Board relied does not establish that the ’872 Patent monitors non-attack activity. The Board therefore both relied-on arguments PO never presented and misapprehended the relevant disclosure.

C. The Board Misunderstood Dr. Jakobsson’s Testimony

Finally, the Board misunderstood Dr. Jakobsson’s testimony relevant to Claim 2. The Board concluded that his testimony “does not persuasively support Petitioner’s position that the disclosed monitoring excludes other activity.” FWD, 21. In fact, Dr. Jakobsson consistently testified that the ’872 Patent describes monitoring only attack activity and that this approach is consistent with the standard operation of honeypots. Dr. Jakobsson’s initial declaration explained that the ’872 Patent allows attackers to attack a decoy network device so that the pattern of the attack can be monitored to generate a fingerprint used to prevent similar future attacks. Ex. 1003, ¶69. He explained this is consistent with known honeypot systems,

which monitor all activity under the assumption that it is all unauthorized. *Id.* at ¶¶49-54, 146.

On cross examination, Dr. Jakobsson confirmed that “all activity is attacker activity” in the context of monitoring decoy devices. Ex. 2053, 116:16-18. This view is supported by Dr. Stavrou, who confirmed that “some embodiments . . . monitor[] all activity on the [VM]” because “all activity on the [VMs] is shown to be unauthorized[.]” Ex. 1034, 136:21-25; Ex. 2031, ¶ 69 (describing the ’872 Patent’s monitoring “*unauthorized activity*”).

Dr. Jakobsson confirmed in his supplemental declaration that both Capalik and the ’872 Patent “run[] VMs that are intentionally left susceptible to attacks, so attacks to the VMs can be monitored.” Ex. 1035, ¶8. He explained that “monitoring occurs in response to attack activity within the VM.” *Id.* Finally, he expressly rejected the notion that the decoy system of the ’872 Patent is “designed to monitor or identify non-attack activity in isolation from a detected attacker access.” *Id.*

The Board nevertheless concluded that “Dr. Jakobsson does not testify that the ’872 patent teaches an absence of non-attack activity on the virtual machine.” FWD 20-21. However, this framing addresses a different question. Petitioner’s position does not depend on proving that only attack activity occurs. Petitioner’s position is that a POSITA would have understood, based on the intrinsic record, that

the activity *monitored* is attack activity. This is the only type of monitoring described, and it is consistent with the nature of honeypot systems known in the art. On this position, Dr. Jakobsson’s testimony is consistent and clear.

IV. CLAIM 8 – THE BOARD DID NOT ADDRESS THE DISPUTE PRESENTED BY THE PARTIES

As discussed above, the Board must base its decision on arguments presented by the parties. *In re IPR Licensing, Inc.*, 942 F.3d, 1368-69. For Claim 8, the Board erred by overlooking the arguments presented by the Parties when it construed “visually distinguishing at least a subset of the associations” as recited in Claim 8. FWD, 22. Rehearing is appropriate to allow the Board to address the Parties’ actual dispute over the meaning of the term “visually distinguishing.”

The ’872 Patent explains that “***any [] graphical scheme*** can be used to visually distinguish [a] subset of [] associations[.]” Ex. 1001, 12:35-41. Consistent with that disclosure, Dr. Jakobsson explained that “a POSITA would have understood that *King’s* dependency graphs ***visually distinguish a subset of the associations by depicting only malignant associations***[.]” Ex. 1003, ¶¶210, 211.

Dr. Stavrou did not dispute that King’s filtered dependency graph constitutes a graphical scheme or explain why displaying only malignant associations would fall outside the specification’s disclosure. Instead, he relied on claim differentiation. Dr. Stavrou opined that “[i]f ‘visually distinguishing’ entailed only displaying a

subset, then claim 8 would add nothing to claim 7 (which already recites displaying a subset of the activities).” Ex. 2031, ¶83. His objection therefore was that if Claim 8 encompasses King’s graphical presentation, then it would be identical in scope to Claim 7. Petitioner directly addressed that claim differentiation argument, explaining why King’s Fig. 3.2(b), if it were displayed, would satisfy Claim 7 but not Claim 8, and why displaying King’s Fig. 3.2(c) satisfies both claims. Reply, 22-23. Thus, Petitioner explicitly demonstrated Claims 7 and 8 retain different scopes.

PO continued to press its claim differentiation argument in the Sur-Reply, claiming that “by ‘graphically displaying’ a subset of the activities, claim 7 already requires graphically displaying a subset of the associations. Claim 8 requires more.” Sur-Reply, 19. Again, PO did not argue that displaying only a subset of associations is inconsistent with the methods of “visually distinguishing” disclosed by the specification.

The Board did not resolve the claim differentiation dispute. Instead, the Board advanced an argument of its own for PO. While the Board agreed with Dr. Jakobsson that displaying only a subset of associations, as recited in the Petition, “may be a graphical scheme,” it determined that “Dr. Jakobsson does not provide persuasive arguments or evidence that [displaying only a subset of associations] constitutes

‘visually distinguishing at least a subset of the associations’ in view of the ’872 patent’s disclosure.” FWD, 23.

This argument is different than the one the Parties litigated. PO made a claim differentiation argument, that displaying only a subset is not visually distinguishing because it would collapse the distinction between Claims 7 and 8. The Board instead advanced a specification-based argument, concluding that Petitioner failed to show that displaying only a subset constitutes “visually distinguishing” under the disclosure of the specification. PO never advanced that specification-based argument, and Petitioner therefore had no reason to address whether displaying a filtered subset falls within the specification’s open-ended list of graphical schemes for visually distinguishing. Had PO advanced this argument, Petitioner would have addressed the nature of the non-exhaustive list of graphical schemes and built out the record with relevant testimony. The Board therefore did not resolve the claim-construction dispute presented by the Parties and instead rejected Petitioner’s position on a rationale Petitioner had no meaningful opportunity to address.

Rehearing is warranted so that the Board can decide the construction of “visually distinguishing” based on the argument presented in the record.

V. CONCLUSION

Petitioner respectfully requests rehearing on Claims 2 and 8.

Dated: September 11, 2026

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Paul R. Hart

Paul R. Hart, Reg. No. 59,646
Paul.Hart@eriseip.com
Erise IP, P.A.
717 17th St., Suite 1400
Denver, Colorado 80202
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on September 11, 2026, a true and correct copy of the foregoing Petitioner's Request for Rehearing by the Director was served electronically on counsel for Patent Owner at the following address:

gpathmanaban@cgsh.com
cnaples@cgsh.com
speters@cgsh.com
dtodd@cgsh.com
jdirba@smithbaluch.com

BY: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646

COUNSEL FOR PETITIONER