UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET INC.,
Petitioner,

v.

BT AMERICAS, INC.,
Patent Owner.

IPR2019-01325
Patent 7,159,237 B2

Before JESSICA C. KAISER, MONICA S. ULLAGADDI, and SCOTT RAEVSKY, *Administrative Patent Judges.*

KAISER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314; 37 C.F.R. § 42.4

PAN EX1011
Palo Alto Networks v. BT Americas
IPR2023-00888

I. INTRODUCTION

Fortinet Inc. ("Petitioner") requested an *inter partes* review of claims 1–42 (the "challenged claims") of U.S. Patent No. 7,159,237 B2 (Ex. 1001, "the '237 patent"). Paper 1 ("Petition" or "Pet."). BT Americas, Inc. ("Patent Owner")[1] filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted "unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." A decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348 (2018). The decision to institute is "a binary choice—either institute review or don't." *Id.* at 1355.

For the reasons that follow, we do not institute an *inter partes* review of the '237 patent.

II. BACKGROUND

A. Related Proceedings

The '237 patent is asserted in *British Telecommunications plc et al. v. Fortinet Inc.*, 1:18-cv-01018 (D. Del.). Pet. 2; Paper 4, 2. This proceeding is related to IPR2019-01324 in which Petitioner challenges claims of a related patent (U.S. Patent No. 7,895,641 B2).

B. The '237 Patent (Ex. 1001)

The '237 patent relates to dynamic network intrusion monitoring, detection, and response. Ex. 1001, 1:7–9. The '237 patent discloses that

[1] Patent Owner's Mandatory Notice identifies also BT United States LLC and BT Group plc as real parties-in-interest. Paper 4, 2.

system administrators normally do not have time or ability to read through large amounts of constantly-updated audit information. *Id.* at 1:26–29. Resources to continuously monitor hacking activities and look out for new attack tactics, tools, and trends are also limited. *Id.* at 1:29–31. According to the '237 patent, such limitations point to a need for automatic defenses. *Id.* at 1:34–40. Although automatic defenses may work against automated attacks, they are, however, at a disadvantage against an intelligent attack for which an intelligent defense is needed. *Id.* at 1:40–43.

The '237 patent discloses deploying and providing a managed security monitoring service ("MSM service") that monitors a customer's network activity using a probe or sentry system. *Id.* at 1:49–53. The MSM service first collects status data from monitored components. *Id.* at 1:53. The MSM service then filters or analyzes the collected data for activity potentially implicating security concerns. *Id.* at 1:53–55. The MSM service further alerts and transmits information about such activity to trained security analysts working at secure operation centers ("SOCs"). *Id.* at 1:55–57. The MSM service guides the security analysts and customer through an appropriate response and optionally, follow-up. *Id.* at 1:57–59. The MSM service can be customized to accommodate network-specific needs and to reflect feedback. *Id.* at 2:23–26. Figure 1 of the '237 patent is reproduced below.

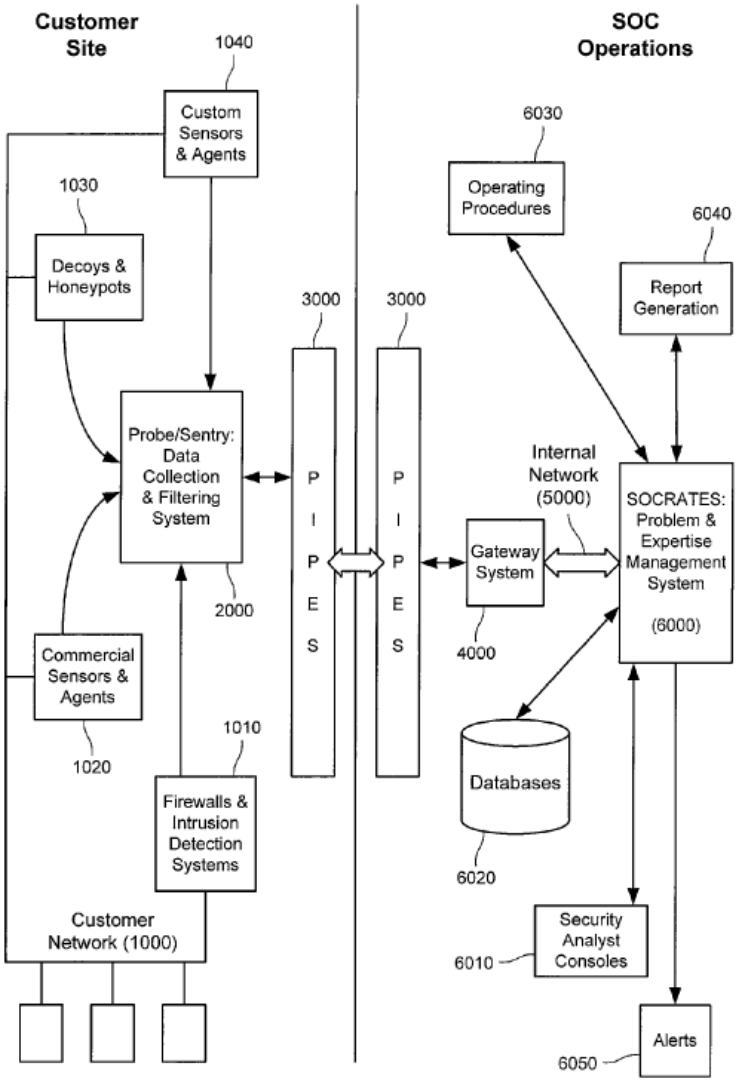


FIG. 1

Figure 1 of the ’237 patent illustrates an overview of the system architecture of an exemplary embodiment.

The ’237 patent discloses that Figure 1 is divided into two portions—components and systems that operate on the customer site (i.e., within the customer’s firewall) and components and systems that operate within the SOC (i.e., within the SOC firewall). *Id.* at 4:38–42. According to the ’237 patent, probe/sentry system 2000, which can be implemented in software or hardware or a combination thereof, monitors sensors attached to customer

network 1000 for evidence of potential security-related events. *Id.* at 4:48–52.

The ’237 patent describes that data collected by sensors 1010, 1020, 1030, and 1040 are filtered by negative filtering subsystem 2020, which discards uninteresting information, and by positive filtering subsystem 2030, which selects potentially interesting information and forwards it to communications and resource coordinator 2060. *Id.* at 8:45–50. Data that is neither discarded by negative filtering subsystem 2020 nor selected by positive filtering subsystem 2030 constitutes “residue,” which is sent to anomaly engine 2050 for further analysis. *Id.* at 8:50–53. Anomaly engine 2050 determines which residue information may be worthy of additional analysis and sends that residue information to communications and resource coordinator 2060 for forwarding to the SOC. *Id.* at 8:53–57. Communications and resource coordinator 2060 creates sentry messages out of interesting status data and forwards the messages to gateway system 4000 via pipes 3000. *Id.* at 8:60–63.

C. Challenged Claims

Claims 1, 18, and 26 are independent. Challenged claims 2–17 depend from claim 1; challenged claims 19–25 depend from claim 18; and challenged claims 27–42 depend from claim 26. Claim 1 is illustrative and is reproduced below.

> 1. A method of operating a probe as part of a security monitoring system for a computer network, comprising:
>
> a) collecting status data from at least one monitored component of said network;
>
> b) analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-

> filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
>
> c) transmitting information about said identified events to an analyst associated with said security monitoring system;
>
> d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and
>
> e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

Ex. 1001, 35:40–57.

D. Proposed Ground of Unpatentability

Petitioner advances the following challenge supported by the declaration of Dr. Narasimha Reddy (Ex. 1003):

Claims Challenged	35 U.S.C. §	Reference(s)
1–42	103	Hill[2] and Warshaw[3]

III. ANALYSIS

A. Claim Construction

For *inter partes* reviews filed on or after November 13, 2018, we apply the same claim construction standard used by Article III federal courts and the ITC, both of which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. 83 Fed. Reg. 51340 (Oct. 11, 2018). Because the instant Petition was filed on July 11, 2019, we apply that standard here. Accordingly, we construe each challenged claim of the'237 patent to generally have "the ordinary and customary meaning of such claim

[2] Ex. 1004, U.S. Patent No. 6,088,084, issued July 11, 2000 ("Hill").
[3] Ex. 1005, Lane B. Warshaw et al., *VenusIDS*: *An Active Database Component for Intrusion Detection*, Applied Research Laboratories / Department of Computer Sciences, The University of Texas at Austin, *Annual Computer Security Application Conference* (1999) ("Warshaw").

as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b).

Petitioner requests "that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding." Pet. 13. Patent Owner contends that Petitioner misconstrues the terms "probe" and "status data," and proposes specific constructions of the aforementioned terms. Prelim. Resp. 39. Patent Owner contends the term "probe" is to be interpreted as a separate element from the Secure Operations Center (SOC). *Id.* at 40–41. Patent Owner contends the term "status data" is to be interpreted as excluding unstructured ASCII data or other data fragments that do not have an independent substantive meaning that bears on status. *Id.* at 42–43.

We construe claim terms to the extent necessary for our analysis on whether to institute a trial. *See, e.g.*, *Nidec Motor Corp. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe 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))). We do not discern a need to construe any claim term to resolve the controversy before us.

B. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art;

(2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). The burden of persuasion never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in an *inter partes* review). Furthermore, Petitioner cannot satisfy its burden of proving obviousness by employing "mere conclusory statements." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

Thus, to prevail in institution of an *inter partes* review, Petitioner must explain how the proposed combinations of prior art would have rendered the challenged claims unpatentable. We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

We review the grounds of unpatentability in view of the understanding of a person of ordinary skill in the art at the time of the invention. *Graham*, 383 U.S. at 17. Petitioner contends that

> [A] POSITA [person of ordinary skill in the art] in March 2000 would have been familiar with intrusion detection systems for

> computer networks. FT-1003 ¶24. A POSITA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor's degree in computer science, computer communications, electrical engineering, or equivalent degree, coupled with four years of experience; or by obtaining a Master's degree in computer science, computer communications, electrical engineering or equivalent field but having two years of experience; or by having no formal education but experience in computer science or computer communications of at least six years.

Pet. 14 (citing Ex. 1003 ¶ 24).

Patent Owner indicates that "[i]n responding to the Petition, and for that purpose alone, Patent Owner accepts the level of ordinary skill presented by Petitioner and applies it to the analysis of obviousness." Prelim. Resp. 38 (citing Pet. 14).

We determine on the current record that the level of ordinary skill proposed by Petitioner is consistent with the '237 patent and the asserted prior art. We adopt that level in deciding whether to institute trial.

D. Obviousness over Hill and Warshaw

Petitioner contends that claims 1–42 are unpatentable under 35 U.S.C. § 103 as obvious over Hill and Warshaw. Pet. 23–73. For the reasons that follow, we are not persuaded that Petitioner has established a reasonable likelihood of prevailing with respect to this ground.

1. Overview of Hill

Hill concerns adaptively responding to computer network security attacks. Ex. 1004, 1:7–9. Hill's system includes multiple security agents that concurrently detect security events on associated computer nodes. *Id.* at 3:20–24. The system includes a processor that processes the security events to form an attack signature. *Id.* at 3:24–26. The system also includes a network status display that displays attack status information representing an

attack. *Id.* at 3:26–30. The processor is trained to compare the attack signature to each of a set of training signatures to determine which of the simulated attacks matches most closely with the attack. *Id.* at 3:30–36. Figure 5 of Hill is reproduced below.

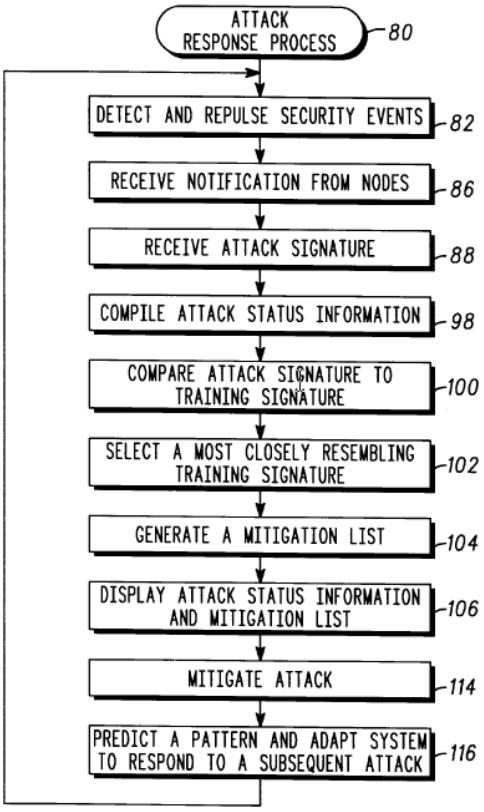


FIG. 5

Figure 5 shows a flowchart of an attack response process performed by the dynamic network security system.

Hill discloses an attack response process 80 that is initiated by a network administrator and that continually responds to security attacks on network 22. *Id.* at 7:61–63. Attack response process 80 begins with task 82, where task 82 detects and repulses security events 50 at nodes 24, and where task 82 is performed concurrently and autonomously at each of nodes 24. *Id.* at 7:64–67. In response to task 82, task 86 is performed through each of

security agents 36, where task 86 causes SOM processor 40 to be notified of an outcome of the repulsing tasks through a security agent 36 associated with a corresponding node 24. *Id.* at 8:4–7. Following notification task 86, task 88 causes SOM processor 40 to receive an attack signature for an attack (*i.e.*, attack signature 94). *Id.* at 8:10–13. In conjunction with receiving task 88, a task 98 compiles attack status information regarding first attack 92. *Id.* at 8:30–32. Following task 98, SOM processor 40 performs task 100, where SOM processor 40 compares a vector representative of first attack signature 94 to each of training signatures 53 as mapped in a display map 66. *Id.* at 8:36–37. In response to comparing task 100, task 102 selects one of training signatures 53 that most closely matches first attack signature 94. *Id.* at 8:40–42. In conjunction with task 102, task 104 generates a mitigation list. *Id.* at 8:50–51. Following tasks 102 and 104, task 106 displays attack status information and the mitigation list on network status display 42. *Id.* at 8:59–61. In response to task 106, task 114 mitigates first attack 92. *Id.* at 9:26–27. Following task 114, task 116 predicts a pattern for subsequent attacks and adapts security system 20 to respond to subsequent attacks. *Id.* at 9:35–37.

2. Overview of Warshaw

Warshaw describes a two-layered network intrusion detection system consisting of a network layer and an analysis layer. Ex. 1005, 2. The network layer includes an array of protected subnetworks. *Id.* A privileged computer on each subnetwork, disclosed in Warshaw as a probe, sniffs network traffic, and executes an initial set of filters that analyze traffic and captures suspicious packets. *Id.* The analysis layer comprises a central Oracle database and the mechanism to identify and report intrusions. *Id.* At the analysis layer, an automated program searches for possible intrusions

patterns and raises alarms for human network analysts if suspicious activity is detected. *Id.* Figure 1 of Warshaw is reproduced below.

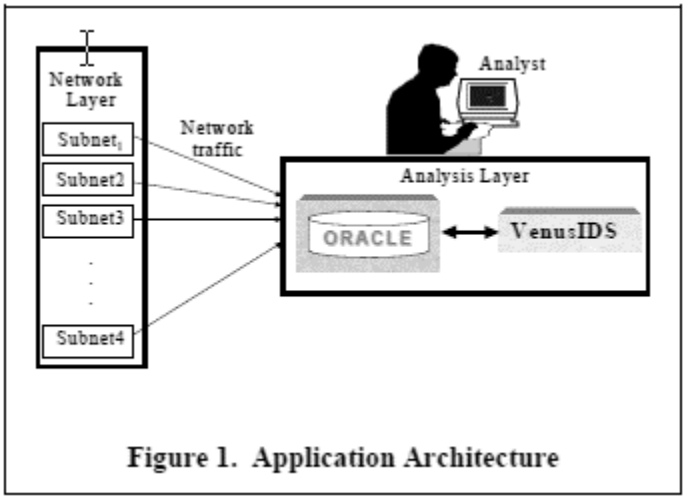


Figure 1 shows an application architecture of a network intrusion detection system.

Warshaw discloses that the network layer includes an array of subnetworks each monitored by a probe. *Id.* A probe sniffs all network traffic on a subnetwork and filters the traffic by discarding obviously non-threatening traffic and classifying the remaining traffic as suspicious or uncertain. *Id.* Suspicious data is logged to the analysis layer in real-time, whereas uncertain data is logged to the analysis layer at predetermined intervals. *Id.*

3. Independent Claim 1

Claim 1 recites, *inter alia,* "analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." In its discussion of the challenge over Hill and Warshaw, Petitioner presents two theories—a first in which Hill alone teaches the above-quoted filtering subsystem limitation, and a second in which

Warshaw teaches a portion of the limitation, the post-filtering residue and an analysis thereof. *See* Pet. 38–44.

(a) Petitioner's Contentions

With respect to its first theory, Petitioner contends:

> A POSITA understood that Hill performs *negative filtering* on the collected status data from the security agents by discarding status data that does not identify a security event. A POSITA also understood that Hill performs *positive filtering* by comparing (i) security event data from the sensor agents that include an attack signature with (ii) the previously stored training signatures. A POSITA understood that Hill discloses the claimed *post-filtering residue data* as an attack signature that does not match a training signature. Hill discloses that "not all possible combinations of events types to produce all possible types of simulated attacks" are included as training signatures. FT-1004 7:49-51. Thus, a POSITA understood that any attack signature that does not match a training signature would be post-filtering residue that requires further evaluation by the network manager.

Pet. 39–40 (citing Ex. 1003 ¶ 103) (emphases added).

With respect to its second theory, Petitioner contends:

> To the extent that Patent Owner argues that Hill does not disclose this limitation, it would be obvious to modify Hill in view of Warshaw to include the recited filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering. Warshaw discloses analyzing traffic to identify and report intrusions (*to identify potentially security-related events*).

Id. at 40. Petitioner quotes the following portion of Warshaw as teaching the portions of the filtering subsystem limitation it acknowledges in this theory are missing in Hill:

> A probe sniffs, in real time, all network traffic on a subnetwork and filters the traffic by discarding obvious non-threatening traffic and classifying the remaining traffic as suspicious or uncertain. Suspicious traffic, also called events, is logged in real-

> time to the analysis layer, while all non-discarded traffic is logged at predetermined intervals to the analysis layer.

Pet. 41–42 (quoting Ex. 1005, 3).

As rationale for modifying Hill with Warshaw, Petitioner presents the following contentions.

First, Petitioner contends that the ordinarily skilled artisan would have been motivated "to reduce the amount of data being analyzed by discarding data that does not indicate a security event and thereby reduce the amount of data to be analyzed by a human, which was a stated goal of intrusion detections systems at the time of the '237 Patent." Pet. 41 (citing Ex. 1006, 7–8).

Second, Petitioner contends that Hill provides express motivation for the combination because "Hill describes that a POSITA understood that the criteria for determining a match between an attack signature and a training signature could rely on other factors[.]" *Id.* at 41–42 (quoting Ex. 1004, 8:45–49) (citing Ex. 1003 ¶ 105). The cited portion of Hill discloses that "other factors will contribute to the selection of a most closely resembling training signature," including, for example, "the location identifiers for each of the affected nodes, network hierarchy, and so forth." Ex. 1004, 8:45–49.

Third, Petitioner contends that Hill provides express motivation for the additional reason that "a new attack signature could become a training signature in subsequent analyses[.]" Pet. 42 (quoting 1004, 9:36–46) (citing Ex. 1003 ¶ 106). Based on Petitioner's second and third contentions, Petitioner argues

> Hill teaches it is beneficial to treat a first attack signature that does not match a previously stored training signature as post-filtering residue (it was neither discarded, nor matched an existing training signature) that is worthy of further analysis

> because it may be added to the security system as a new training signature to help identify security events in subsequent analysis to help the security system evolve with evolving threats.

Id. (citing 1003 ¶ 107).

Fourth, Petitioner contends that the ordinarily skilled artisan would have been motivated to combine Hill and Warshaw because both references are directed to or disclose: (1) "monitoring components of a computer network to detect and prevent intrusions"; (2) "systems that facilitate a human analyst's review of data received from monitored components to detect intrusions and identify problem resolution"; (3) "a multilayer approach of collecting information at the component level and forwarding the information to an analysis layer"; and (4) "architectures and methods that allow for substantially real-time detection." *See id.* at 42–43.

(b) Patent Owner's Contentions

According to Patent Owner, "[t]here is not the slightest suggestion," in Hill, "that residue status data is analyzed or that any analysis is performed to identify potentially security-related events before transmission to processor 40." Prelim. Resp. 47 (citing Ex. 2001 ¶¶ 102–105). Patent Owner argues that "Petitioner's own expert admits that there is no actual discussion of filtering status data in Hill, much less into residue, and just provides his opinion that a POSITA would understand implicitly what Hill does not expressly state or suggest," which should "carr[y] no weight in this regard." *Id.* at 48 (citing 1003 ¶ 103[4]; 37 C.F.R. § 42.65(a); *Magnum Oil Tools*, 829 F.3d at 1380; *ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012)).

[4] We understand Patent Owner's citation to Paragraph 1003 to be a typographical error.

Patent Owner further contends that "[t]here is no indication that the Warshaw authors filtered status data and, once again, not the slightest suggestion that residue status data is analyzed at the probe to identify a potential event." *Id.* at 47–48 (citing Ex. 2001 ¶¶ 122–130). According to Patent Owner, "Warshaw transmits not only everything that was bad ('suspicious'), but also transmits everything that was indeterminate ('uncertain'), to the analysis layer." *Id.* at 48 (citing Ex. 1005, 3).

Patent Owner disputes Petitioner's rationale for modifying Hill with Warshaw and Dr. Reddy's testimony that "a desire to discard data to reduce the amount of data to be analyzed by humans would provide motivation . . . because Warshaw does not provide any suggestion how to reduce traffic, choosing instead to manage the flow of traffic" by sending all but the "non-threatening" class of traffic to the analysis layer. *See id.* at 53–54 (citing Ex. 1003 ¶ 105; Ex. 1005, 3; Ex. 2001 ¶ 137). Patent Owner contends Warshaw does not provide guidance on how to modify Hill because "Warshaw does not filter status data, does not advocate the use of filtering status data, and does not provide nearly enough detail as to what it is doing, much less how, to suggest to anyone a mechanism for modifying Hill with any expectation of improvement or success." *Id.* at 54–55 (citing Ex. 2001 ¶ 164).

Patent Owner further contends that "the architecture of Hill does not allow itself to be modified to arrive at the invention" because Hill's processor 40 has to be trained in order to recognize attack signatures in traffic and because Hill's system cannot "conduct a second, deeper level of analysis . . . because there are no security analysts with tools and databases at their disposal." *Id.* at 54 (citing Ex. 2001 ¶¶ 22, 106, 113, 117, 162).

(c) Discussion of Petitioner's First Theory

With respect to its first theory, Petitioner cites Hill's teaching of matching "security event data . . . that include[s] an attack signature" to "previously stored training signatures" as teaching the claimed "data . . . selected by filtering" (i.e., positive filtering), "data . . . discarded . . . by filtering" (i.e., negative filtering), *and* "post-filtering residue [that] is neither discarded nor selected by filtering." *See* Pet. 39–40. The cited portions of Hill do not teach or suggest discarding data not matching a training signature, contrary to Petitioner's contention. Petitioner's argument that "[a] *POSITA understood* that Hill performs *negative filtering* on the collected status data from the security agents by discarding status data that does not identify a security event" is similarly unsupported by evidence. *Id.* (certain emphasis added).

So too is Petitioner's argument that "a *POSITA understood* that any attack signature that does not match a training signature would be post-filtering residue that *requires further evaluation by the network manager*." *Id.* at 40 (emphases added). Petitioner does not explain sufficiently how Hill would have been understood to disclose discarding status data that does not identify a security event, and at the same time, retaining data that includes an as yet unmatched attack signature. Dr. Reddy's testimony does little to explain or further support Petitioner's position. *See* Ex. 1003 ¶ 103. Apart from explaining how Hill would have been understood by the ordinarily skilled artisan to disclose the general concept of filtering, the Declaration does little more than repeat the arguments spanning pages 39 and 40 of the Petition. *Compare* Pet. 39–40, *with* Ex. 1003 ¶ 103; *see* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

For the foregoing reasons, we are not persuaded that Petitioner shows sufficiently that Hill alone teaches "post-filtering residue," let alone "an analysis of post-filtering residue" as recited in the analyzing status data limitation.

(d) Discussion of Petitioner's Second Theory

As set forth above, Petitioner takes the alternative position that "it would be obvious to modify Hill in view of Warshaw to include the recited filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." Pet. 40. Petitioner further contends "Warshaw discloses analyzing traffic to identify and report intrusions (to identify potentially security-related events). The identifying includes negative filtering which results in data being discarded, positive filtering which results in data being selected and classified as suspicious, and post filtering of residue data that is neither discarded or classified as suspicious." *Id.* at 40–41. As discussed above, Warshaw discloses:

> A probe sniffs, in real time, all network traffic on a subnetwork and filters the traffic by discarding obvious non-threatening traffic and classifying the remaining traffic as suspicious or uncertain. Suspicious traffic, also called events, is logged in real-time to the analysis layer, while all non-discarded traffic is logged at predetermined intervals to the analysis layer.

Ex. 1005, 3. We are not persuaded, however, that Petitioner's rationale for combining Hill and Warshaw is supported by sufficient rational underpinning for the reasons that follow.

With respect to Petitioner's first contention that a person of ordinary skill in the art would have been motivated to modify Hill to discard certain data in order to reduce the volume of human analysis (*see* Pet. 41 (citing Ex.

1006, 7–8)), it is not clear to us that data requiring human analysis would be reduced as a result of the combination. In addition, it is not clear from the cited portions that Hill discloses that a human performs analysis on data not implicating a security event.

With respect to Petitioner's second contention that Hill provides express motivation for the combination, the cited portion of Hill discloses that "other factors will contribute to the *selection of a most closely resembling training signature*," including, for example, "the location identifiers for each of the affected nodes, network hierarchy, and so forth." Ex. 1004, 8:45–49 (emphasis added). It is not clear how this portion of Hill would have motivated one of ordinary skill in the art to modify Hill to discard data as Petitioner contends is taught by Warshaw. It is further unclear how Warshaw's teachings might constitute Hill's "other factors." The cited portion of Hill concerns other factors to consider in conjunction with *positive* filtering. *See id.* It does not convey why the ordinarily skilled artisan would have modified Hill to add the *negative filtering*, post-filtering residue data, or an analysis of the post-filtering residue data that Petitioner contends is taught by Warshaw.

Petitioner's third contention that Hill provides express motivation for the additional reason that "a new attack signature could become a training signature in subsequent analyses" is an argument why Hill *alone* teaches all elements of the filtering subsystem limitation. *See* Pet. 42 (quoting Ex. 1004, 9:36–46) (citing Ex. 1003 ¶ 106). Petitioner points to Hill as teaching that "it is beneficial to treat a first attack signature that does not match a previously stored training signature as post-filtering residue (it was neither discarded, nor matched an existing training signature) that is worthy of further analysis[.]" *Id.* (citing Ex. 1003 ¶ 107). Petitioner does not discuss

Warshaw's teaching in relation to this purported express motivation in Hill. *See id.* We have already discussed in the preceding section why we are not persuaded that Hill alone teaches the filtering subsystem limitation in its entirety. We also note that Petitioner does not explain adequately why this teaching in Hill is not, at most, further actions taken with positively filtered data in Hill (i.e., Hill identifies these as attack signatures and then takes further action after mitigation to improve its list of training signatures). *See* Ex. 1004, 8:40–61, 9:35–46.

With respect to Petitioner's fourth contention that Hill and Warshaw disclose common features, we consider this an argument that the references are analogous art. *See* Pet. 42–43. On its own, Petitioner's analogous art argument is insufficient to sustain a rationale for combining Hill and Warshaw. Merely asserting that these prior art references are analogous art to each other is not a sufficient articulated reason with a rational underpinning to combine their respective teachings. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); *see also Securus Techs., Inc. v. Global Tel*Link Corp.*, 701 Fed. App'x 971, 977 (Fed. Cir. 2017) ("We agree with the Board that a broad characterization of [the references] as both falling within the same alleged field of 'telecommunications monitoring and control,' without more, is not enough for [Petitioner] to meet its burden of presenting a sufficient rationale to support an obviousness conclusion."). As we are not persuaded by any of Petitioner's other contentions, we determine that Petitioner's fourth contention is unpersuasive as insufficient to support Petitioner's rationale for combining Hill and Warshaw.

For the foregoing reasons, we are not persuaded that Petitioner establishes a reasonable likelihood of prevailing in demonstrating that

independent claim 1 is unpatentable as obvious over the combination of Hill and Warshaw.

4. Independent Claim 18

Claim 18 recites, *inter alia*, "at least one probe, wherein said probe is configured to . . . analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." Petitioner relies on the same contentions and arguments as presented with respect to independent claim 1. *See* Pet. 64 (citing Ex. 1003 ¶ 140) ("Hill and Warshaw disclose this limitation for the same reasons as discussed with respect to limitation 1(b).").

For substantially the same reasons set forth above with respect to independent claim 1, we are not persuaded that Petitioner establishes a reasonable likelihood of prevailing in demonstrating that independent claim 18 is unpatentable as obvious over the combination of Hill and Warshaw.

5. Independent Claim 26

Claim 26 recites, *inter alia*, "analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." Petitioner relies on the same contentions and arguments as presented with respect to independent claim 1. *See* Pet. 68 (citing Ex. 1003 ¶ 151) ("Claim 26 is a computer program claim corresponding to the method recited in Claim 1. Hill and Warshaw disclose this claim for the same reasons as discussed with respect to Claim 1.").

For substantially the same reasons set forth above with respect to independent claim 1, we are not persuaded that Petitioner establishes a reasonable likelihood of prevailing in demonstrating that independent claim 26 is unpatentable as obvious over the combination of Hill and Warshaw.

6. Dependent Claims 2–17, 19–25, and 27–42

As Petitioner has not demonstrated a reasonable likelihood of prevailing in its challenge of unpatentability of independent claims 1, 18, and 26, we determine that Petitioner also has not demonstrated a reasonable likelihood of prevailing with respect to its challenge to dependent claims 2–17, 19–25, and 27–42.

E. 35 U.S.C. § 325(d)

Patent Owner argues that we should exercise discretion to deny the Petition under 35 U.S.C. § 325(d). Prelim. Resp. 56–65. Petitioner argues that we should not. Pet. 21–22. As we deny institution on the merits of Petitioner's challenge to claims 1–42 applying Hill and Warshaw, we need not address arguments relating to 35 U.S.C. § 325(d).

IV. SUMMARY

We determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing in demonstrating that any of claims 1–42 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Hill and Warshaw.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the petition for *inter partes* review is *denied* and no trial is instituted.

FOR PETITIONER:

Patrick McPherson
Christopher Tyson
Patrick Muldoon
D. Joseph English
DUANE MORRIS LLP
pdmcpherson@duanemorris.com
cjtyson@duanemorris.com
pcmuldoon@duanemorris.com
djenglish@duanemorris.com

FOR PATENT OWNER:

James Shalek
Anthony Coles
Evan Kahn
Nolan Goldberg
Gerald Worth
PROSKAUER ROSE LLP
jshalekptabmatters@proskauer.com
acoles@proskauer.com
ekahn@proskauer.com
ngoldberg@proskauer.com
gworth@proskauer.com