

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,
Petitioner,

v.

SECURITYPROFILING, LLC,
Patent Owner.

Case IPR2017-02192
Patent 8,984,644 B2

Before BRIAN J. McNAMARA, GREGG I. ANDERSON, and
MINN CHUNG, *Administrative Patent Judges*.

ANDERSON, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
INTER PARTES REVIEW
35 U.S.C. § 318(a) AND 37 C.F.R. § 42.73

I. INTRODUCTION

Trend Micro, Inc. (“Petitioner”) filed a Petition (“Pet.” (Paper 1)) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1, 7, and 14 (“the challenged claims”) of U.S. Patent No. 8,984,644 B2 (“the ’644 patent” (Ex. 1001)). SecurityProfiling, LLC (“Patent Owner”)

filed a Preliminary Response (“Prelim. Resp.” (Paper 6)). On April 11, 2018, we instituted trial on all challenged claims but on fewer than all grounds. (“Institution Decision,” “Inst. Dec.,” Paper 7).

On April 24, 2018, the United States Supreme Court held that 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, 1359–60 (2018). Following *SAS*, the U.S. Patent and Trademark Office (“Office”) issued “Guidance on the impact of *SAS* on AIA trial proceedings,” in which the Office took the policy position that a decision granting institution will institute on all of the challenged claims in the petition *and* the review will include all challenges to those claims presented in the petition.¹ The U.S. Court of Appeals for the Federal Circuit endorsed this Office policy by explaining that “‘the petitioner’s petition, not the Director’s discretion, is supposed to guide the life of the litigation,’ and ‘that the petitioner’s contentions, not the Director’s discretion, define the scope of the litigation all the way from institution through to conclusion.’” *Adidas AG v. Nike, Inc.*, 894 F.3d 1256, 1258 (Fed. Cir. 2018) (citations omitted) (quoting *SAS*, 138 S. Ct. at 1356–1357). In accordance with *SAS* and Office policy, we modified our Institution Decision (“Modified Institution Decision,” “Mod. Inst. Dec.,” Paper 10) to include review of all grounds presented by Petitioner in its Petition. In response to the Modified Institution Decision, the parties stipulated that “no additional briefing and no schedule change is necessary in IPR2017-02192.” Paper 14.

¹ “Guidance on the impact of *SAS* on AIA trial proceedings” (April 26, 2018), <https://www.uspto.gov/patents-application-process/patent-trial-and-appeal-board/trials/guidance-impact-sas-aia-trial>.

Patent Owner filed a Response (“PO Resp.,” Paper 19) and Petitioner filed a Reply (“Pet. Reply,” Paper 21). At Patent Owner’s request, we authorized Patent Owner’s filing of a Sur-Reply (“PO Sur-Reply,” Paper 23) directed to an alleged new argument made in the Petitioner’s Reply. See Paper 22.

The Petition is supported by the Declaration of Seth James Nielson, Ph.D. (“Nielson Declaration,” Ex. 1011). The Response is supported by the Declaration of Nick Feamster Ph.D. (“Feamster Declaration,” Ex. 2005). The parties present the Nielsen and Feamster Declarations as the testimony of experts. See Fed. R. Evid. 702. As evidence supporting its asserted date of invention, Patent Owner further relies on the Declaration of John Blignaut Under 37 C.F.R. § 1.131 (“Blignaut Declaration,” Ex. 2001) and the Declaration of Brett Young Under 37 C.F.R. § 1.131 (“Young Declaration,” Ex. 2006). None of the declarants were deposed. An oral hearing was held on January 16, 2019, and a transcript of the hearing is included in the record (“Tr.,” Paper 30).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of claims 1, 7, and 14 of the ’644 patent. For the reasons discussed below, we hold that Petitioner has demonstrated by a preponderance of the evidence that claims 1, 7, and 14 are unpatentable under §§ 102, 103.

II. BACKGROUND

A. *Related Proceedings*

Petitioner advises that the ’644 patent has been asserted in the following district court litigations: *SecurityProfiling, LLC v. Trend Micro America, Inc. and Trend Micro, Inc.*, Case No. 3:17-cv-01484(N.D. Tex.);

and *SecurityProfiling, LLC v. Intel Corporation et al.*, Case No. 6:16-cv-01016 (E.D. Tex.) (dismissed June 8, 2017). Pet. 13–14; Paper 5, 1–2.

The parties also identified a petition for *inter partes* review with respect to U.S. Patent No. 8,266,699, which claims priority to U.S. Provisional Application No. 60/484,085, to which the '644 patent also claims priority. Pet. 10; Paper 5, 2; see *Trend Micro, Inc. v. SecurityProfiling, LLC*, IPR2017-02191 (“’2191 IPR”).²

B. Technology and the '644 Patent (Ex. 1001)

The '644 patent relates generally to computer systems and specifically to management of security of computing and network devices. Ex. 1001, 1:19–21.

1. Background Technology

The '644 patent explains that “[t]he latest network compromises are combining qualities of viruses, worms, and denial of service attacks into new blended attacks.” Ex. 1001, 8:9–11.

To mitigate these new risks, organizations deploy a multi-tiered network defense strategy comprised of a variety of additional network security products layered at the perimeter and to internal network machines and devices. Such network security products include antivirus, firewall, scanners, and network and host based intrusion detection systems.

Ex. 1001, 10:24–29. However, the multi-tiered network defense strategy has drawbacks that the '644 patent purports to address. *Id.* at 10:56–65.

² Terminated per Patent Owner’s Request for Adverse Judgment. See ’2191 IPR Papers 17, 18.

2. *The '644 Patent*

According to the Summary in the '644 patent specification, the invention identifies “a first and second occurrence in connection with at least one of the networked device.” Ex. 1001, 1:25–27. As explained in Section II.B.2, on this record and for the purposes of this decision, we construe “occurrence” as “an event that seeks to take advantage a vulnerability, such as an attack by a virus or worm or the like.”

[I]t is determined that the at least one actual vulnerability of the at least one networked device is capable of being taken advantage of by the first occurrence identified in connection with the at least one networked device. . . . [T]he at least one actual vulnerability of the at least one networked device is not capable of being taken advantage of by the second occurrence identified in connection with the at least one networked device. To this end, the first occurrence and the second occurrence are reported differently.

Id. at 1:28–37.

The Detailed Description of the '644 patent describes at a high level how the invention relates to problems associated with multi-tiered network defenses.

In one embodiment, technology may integrate with and enable network security products to intelligently reference and share information from the same vulnerability data set, provide vulnerability identification and remediation functionalities, and efficiently meet policy compliance and enforcement requirements.

Ex. 1001, 11:8–14; *see also id.* at 13:46–67 (describing “vulnerability management” in similar terms). The '644 patent describes approximately fifteen different embodiments ostensibly relating to solving issues

surrounding multi-tiered defenses and “vulnerability management.” *Id.* at 11:4–14:8.

C. Challenged Claims

As noted above, Petitioner challenges claim 1 of the ’644 patent, which is an independent computer program product claim, from which claims 7 and 14 depend. Claim 1 is the only independent claim of the ’644 patent. We adopt Petitioner’s notation for the claims where the claim is followed by a letter designations for each limitation. *See, e.g.,* Pet. 42. Using Petitioner’s notation, claim 1 is reproduced below as representative:

- 1.a. A computer program product embodied on a non-transitory computer readable medium, comprising:
 - b. code for receiving actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including:
 - c. at least one first potential vulnerability, and at least one second potential vulnerability;
 - d. said actual vulnerability information generated utilizing the potential vulnerability information, in response to code execution by at least one processor, by:
 - identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and
 - determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities;

- e. code for identifying an occurrence in connection with at least one of the plurality of devices;
- f. code for determining that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the actual vulnerability information; and
- g.³ code for providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.

Ex. 1001, 31:23–60.

D. Instituted Grounds of Unpatentability

Petitioner asserted the following grounds of unpatentability under 35 U.S.C. §§ 102 and 103. Pet. 17. We instituted trial on all grounds. Inst. Dec. 42–43; Mod. Inst. Dec. 2–3.

³ Patent Owner and its expert refer to limitation 1.g as limitation 1.8. See Pet. 39; PO Resp. 51–52; Ex. 2005 ¶ 32 (pg. 39). Petitioner’s expert uses limitation 1[e] for the same limitation. See Ex. 1011 ¶ 61. For purposes of this Decision, we use Petitioner’s designation for this Decision. The same disparity is present for limitation 1.d which Patent Owner refers to as 1.4. See Pet. 43; PO Resp. 44. Where helpful to clarify, we use both designations, e.g., 1.d/1.4.

Ground	Reference[s]	Basis	Claim[s] Challenged
1	Shah ⁴	§102(a)(1) ⁵	1
2	Shah and Hill ⁶	§103	7
3	Gupta ⁷ and Girouard ⁸	§103	1, 7, 14
4	Gleichauf ⁹ and Hill	§103	1, 7, 14

III. ANALYSIS

A. Prior Art Status of Shah and Girouard

Patent Owner contends that Shah and Girouard are not prior art because the claimed subject matter of the '644 patent was invented prior to the respective filing dates of the references, i.e., May 22, 2003, and September 30, 2002. *See* PO Resp. 26 (citing Ex. 1002; Ex. 1005). Patent

⁴ Paragi Shah *et al.*, US 2004/0073800 A1, filed May 22, 2003, published April 15, 2004 (“Shah,” Ex. 1002).

⁵ Petitioner contends that the challenged claims are governed by the Leahy-Smith America Invents Act (AIA), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011). Pet. 32. The AIA revised 35 U.S.C. §§ 102 and 103 and became effective March 16, 2013. AIA § 3(n)(1)2. Under the AIA, first to file governs novelty. Pet. 28–29; *see also* 35 U.S.C. § 102 (a) (AIA) (prior art must be “effectively filed before the effective filing date of the claimed invention.”).

⁶ Douglas W. Hill, *et al.*, US Patent No. 6,088,804, filed January 12, 1998, issued July 11, 2000 (“Hall,” Ex. 1003).

⁷ Ramesh M. Gupta, *et al.*, US 2003/0004689 A1, filed June 13, 2002, published January 2, 2003 (“Gupta,” Ex. 1004).

⁸ Mario Girouard, US 2004/0064726 A1, filed September 30, 2002, published April 1, 2004 (“Girouard,” Ex. 1005).

⁹ Robert E. Gleichauf, *et al.*, US Patent No. 6,301,668, filed December 29, 1998, issued October 9, 2001 (“Gleichauf,” Ex. 1006).

Owner argues that the effective filing date of the application for the '644 patent was prior to March 16, 2013, the effective date of the AIA and, therefore, the AIA's first inventor to file framework does not apply to the challenged claims. *Id.* at 23.

1. Applicable Law Relating to Written Description Support to Obtain Benefit of Earlier Filing Date

In order to be entitled to the benefit of the filing date of an application previously filed, the earlier filed application must be “disclosed in the manner provided” by section 112. 35 U.S.C. § 120. Section 112 requires

a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

35 U.S.C. § 112(a) (2012); *accord* § 112 ¶ 1 (2006) (pre-AIA version).

Determining whether Patent Owner may claim the benefit of the previously filed applications requires us to compare the claims “with the invention disclosed in the specification, and if the claimed invention does not appear in the specification . . . the claim . . . fails regardless of whether one of skill in the art could make or use the claimed invention.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc)). “[T]he test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art.” *Ariad*, 598 F.3d at 1336. Generic language insufficient to satisfy the written description requirement. *Id.*

Where the field “is a predictable art . . . a lower level of detail is required to satisfy the written description requirement than for unpredictable

arts.” *Hologic, Inc. v. Smith & Nephew, Inc.*, 884 F.3d 1357, 1361 (Fed. Cir. 2018). Claims that exceed the scope of the subject matter the inventor disclosed are invalid for failure to meet the written description requirement. *Atlantic Res. Marketing v. Troy*, 659 F3d 1345, 1355 (Fed. Cir. 2011). A description that merely renders the invention obvious does not satisfy the requirement. *Lockwood v. Am. Airlines*, 107 F.3d 1565, 1571–72 (Fed. Cir. 1997).

2. Issue and Summary of Parties’ Arguments

The issue we must decide is whether each application in the ’644 chain of previously filed applications leading back to the earliest filed application complies with the statutory written description requirement under section 112, entitling the ’644 patent to the benefit of the filing date of a previously filed application under section 120. The chain of previously filed applications leading up to the application for the ’644 patent is shown in the table below.

Chain of Applications

Application	Filing Date	Description/Status
No. 60/484,085 (“Provisional,” “’085 application,” Ex. 1008/Ex. 2003) ¹⁰	July 1, 2003	Earliest filed application.
No. 10/882,852 (“’852 application,” Ex. 1009)	July 1, 2004	Abandoned.
No. 14/138,014 (“’014 application,” Ex. 1010)	Dec. 21, 2013	Continuation of ’852 application.
No. 14/499,237 (“’237	Sept. 28,	Continuation-in-part of ’014

¹⁰ We credit the un rebutted testimony from the Nielson Declaration, that the ’085 application, “appears to be largely comprised of SecurityProfiling marketing and product documents.” Ex. 1011 ¶60.

Application	Filing Date	Description/Status
application,” Ex. 1007)	2014	application. Issued as ’644 patent.

Ex. 1001 (60), (63).

Patent Owner argues the ’644 patent should receive the benefit of the July 1, 2003, filing date of the Provisional. PO Resp. 22–25.¹¹ Patent Owner then argues that the July 1, 2003, filing date predates the March 16, 2013, date when the AIA became effective and that pre-AIA section 102 applies. *Id.* at 23. Patent Owner thus seeks to disqualify Shah and Girouard as prior art by demonstrating, “through affidavit or declaration of the patent owner, a date of invention prior to the publication date of the reference (or filing date, for a patent document).” *Id.* at 25–26 (citing 37 C.F.R. § 1.131(a); MPEP §715). If neither Shah nor Girouard are prior art, those grounds relying on Shah or Girouard, i.e., Grounds 1 through 3 of the Petition, must be found in Patent Owner’s favor. *Id.* at 1, 25–26.

Petitioner argues the earlier filed applications do not “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” Pet. 26 (alteration in original) (quoting *Ariad*, 598 F.3d at 1336). Petitioner argues that the subject matter

¹¹ Upon institution, the burden of production shifted to Patent Owner to produce evidence and supporting argument that the ’644 patent is entitled to the priority of the prior filed ’085 application. Inst. Dec. 11 (citing *Dynamic Drinkware, LLC v. Nat’l Geographics, Inc.*, 800 F.3d 1375, 1379 (Fed. Cir. 2015)). Patent Owner acknowledges that it has the burden of production on the priority issue. See PO Resp. 22–23. While Patent Owner has the burden of production, the ultimate burden is always on Petitioner. Inst. Dec. 11 (citing *Dynamic Drinkware*, 800 F.3d at 1379).

of limitation 1.g was not included in any application in the chain until a November 12, 2014, preliminary amendment to the '237 application. *Id.* at 30–32 (citing Ex. 1007, 556–557). Petitioner asserts that, therefore, the earliest priority date for these claims is the September 28, 2014 filing date of the '237 application. *Id.* Petitioner also asserts that because the effective filing date¹² of the '644 patent is September 28, 2014, which is after March 16, 2013, this case must accordingly proceed under the AIA first-to-file provisions. *Id.* at 18, 32.

A second argument, first presented in Petitioner's Reply, is that Patent Owner could not meet its burden to show entitlement to the earlier priority date using incorporation by reference. Pet. Reply 7–8 (citing 37 C.F.R. § 1.57(d)). The Petition relies only on the section 112 issue and Petitioner argues incorporation by reference only because it was raised in the Response. See Pet. Reply 6. Because we determine that neither the Provisional nor the '852 application meets the requirements of section 112, we need not reach Petitioner's incorporation by reference argument. In any case, Patent Owner acknowledges that 37 C.F.R. § 1.57(d) does not apply to claims for priority. See PO Sur-Reply 1–3 (citing *Droplets, Inc. v. E*TRADE Bank*, 887 F.3d 1309, 1319–20 (Fed. Cir. 2018); MPEP 608.01(p) (2018)); Tr. 70:6–14 (arguing “I agree that if we are not entitled to the

¹² “The term ‘effective filing date’ for a claimed invention in a patent or application for patent means—(A) if subparagraph (B) does not apply, the actual filing date of the patent or the application for the patent containing a claim to the invention; or (B) the filing date of the earliest application for which the patent or application is entitled, as to such invention, to a right of priority under section 119, 365(a), 365(b), 386(a), or 386(b) or to the benefit of an earlier filing date under section 120, 121, 365(c), or 386(c).” 35 U.S.C. § 100(i)(1).

priority of the provisional application, then we're out on the prior invention section 1 – the 131 . . . even if we are entitled to the priority of the provisional, we still have to swear back before the provisional to overcome the prior art.”).

3. *Whether the Previously Filed Applications Reasonably Convey to Those Skilled in the Art that the Inventor had Possession of the Claimed Subject Matter as of the Filing Date as Required by Section 112*

Petitioner has shown that the '644 patent is not entitled to the July 1, 2003, filing date of the Provisional. Specifically, we determine that subject matter of limitation 1.g of the '644 patent was not described sufficiently in the Provisional or the '852 application to show applicant was in possession of the invention at the time either application was filed. *Ariad*, 598 F.3d at 1336.

Limitation 1.g recites:

code for providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.

Ex. 1001, 31:51–60. Limitation 1.g is the only limitation challenged as not having written description support. Tr. 11:20–12:16.

Petitioner's argument and evidence with respect to limitation 1.g take two separate tacks with respect to whether the Provisional describes limitation 1.g. The first argument relates to the limitation “providing a user with one or more options to selectively utilize different occurrence

mitigation actions,” also referred to as the “user option” aspect of the claim. *See* Pet. 30. This argument is based primarily on the description contained in the Provisional. The second argument is that the “firewall and intrusion protection options” recited in limitation 1.g are not described in the Provisional. This second argument is presented primarily in the expert testimony of the Nielson Declaration cited in the Petition. *Id.* (citing Ex. 1011 ¶¶ 61, 69¹³).

Starting with the first argument, we find that the Provisional describes an automated process or system and not the claimed “user option.” We agree with Petitioner that

the ’085 Provisional discloses “Anti-Vulnerability applications are transparently integrated, retaining preexisting architecture, processes, and interfaces” and “the end user experience remains the same, or improved with simplified or automated processes.”

Pet. 30 (citing Ex. 1008, 18/Ex. 2003, 11). Specifically, the Provisional does not provide a “user option” but instead “*automatically* deploy[s] the appropriate update to each machine or device.” *Id.* (quoting Ex. 1008, 21 [17]/Ex. 2003, 11); *see also id.* (citing Ex. 1011 ¶¶ 61, 69). Applying the ordinary meaning to the claim language, a “user” is a person who “selectively utilize[s] different occurrence mitigation actions.” Ex. 1001, 31:51–53 (claim 1). This is in contrast to the Provisional’s description of an automated process.

Patent Owner’s arguments also support our finding that the Provisional describes an automated system. *See* PO Resp. 10 (citing

¹³ The Nielsen Declaration includes additional support for Dr. Nielsen’s opinion that the ’085 application does not support this limitation. Ex. 1011 ¶¶ 62–68.

Ex. 2005 ¶ 31 (pp. 24–25) (“This information is shared with the Sensor, Firewall, and other point products, which can then use the information to *automatically* avoid harmful activities.” (emphasis added)); Ex. 2003, 9).¹⁴ Among other citations to the Provisional, Patent Owner and its expert cite to pages 27 and 29 of Exhibit 2003 (Petitioner’s Exhibit 1008 at pages 34 and 36) as describing the functionality of the Provisional and specifically limitation 1.g. PO Resp. 8 (see G.); Ex. 2005 ¶ 32 (see p. 42).

Between pages 27 and 29 cited by Patent Owner, page 28 of Exhibit 2003 describes the SysUpdate™ product of Patent Owner, a description of which is included in the Provisional.¹⁵ See Ex. 1011 ¶ 60. The SysUpdate™ product is also cited in the Feamster Declaration as supporting that the Provisional describes limitation 1.g. See Ex. 2005 ¶ 32 (pg. 40) (“Policy changes may be *automatically* enforced to each computer or device individually, or by group, consistent in accordance with the policy selected

¹⁴ Though not cited by Patent Owner in connection with the priority issue, we have reviewed the prior invention evidence of Patent Owner, including the Blignaut Declaration (Ex. 2001) and the Young Declaration (Ex. 2006). Neither includes facts supporting that a “user option” was present in the alleged prior activities of the inventors. See, e.g., Ex. 2001 ¶ 13 (regarding limitation 1.g); Ex. 2006 ¶ 19.

¹⁵ Although this page of the Provisional was not cited by Petitioner, it supports Petitioner’s argument that the Provisional describes an automatic system and does not provide “user options.” We can consider what is contained in the Provisional in finding that it describes only an automatic solution and does not provide the claimed “user option,” as argued by Petitioner. See *In re NuVasive, Inc.*, 841 F.3d 966, 973 (Fed. Cir. 2016) (Board has “solid basis” for its decision relying on arguments that were advanced by a party and on what was disclosed in a reference) (citing *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016)).

by the network administrator.” (alteration in original) (emphasis added) (quoting Ex. 1008, 34; Ex. 2003, 28)). Page 28 includes six functions of SysUpdate™ system which is described as part of “the first technology to fully automate the updating and reporting processes, as described below.” Ex. 1008, 35; Ex. 2003, 28. Every function listed is described as “automatically” performed. *Id.* A description of the SysUpdate™ product is included as part of the AVT technology described in the Provisional. *See* Ex. 1008, 10/Ex. 2003, 3.

Patent Owner argues in connection with claim 14, which depends from claim 1, “Dr. Feamster states that the user has the opportunity for selecting as user input at the console the option of automatically applying a firewall mitigation system.” Tr. 42:3–9. Patent Owner argued at oral hearing that the Provisional’s disclosure of the “console” described limitation 1.g. *Id.* at 47:7–8, 48:6–22. Patent Owner’s argument made at oral hearing emphasizes that the Provisional describes an automated system. *Id.* at 48:20–22 (“[M]anagement via the console . . . *automates the deployment*, assessment and enforcement of the policy chosen.” (emphasis added)). Patent Owner’s Response asserts “[t]he entire operation is *monitored by the user* via a console, identified as both the ‘Management Console’ and the ‘IDS Console’ (depending on which function was being emphasized at the time).” *See* PO Resp. 8 (citing Ex. 1008, 34, 36/Ex. 2003, 27, 29); *see also* Ex. 2005 ¶ 31 (p. 22 (item H)) (“operation is *monitored* . . . via a console” (emphasis added)). The Response does not specifically address Petitioner’s argument that the Provision only describes an “automatic” selection process. *See* Pet. 30 (the Provisional “*automatically* deploy[s] the appropriate update”).

There is no evidence of record that supports a finding the Provisional Application discloses the “user option,” i.e., “providing a user with one or more options to selectively utilize different occurrence mitigation actions,” as recited in claim 1. None of the cited disclosures from the Provisional or the Feamster Declaration describe clearly, if at all, the “user option.”

Rather, the argument and evidence of Patent Owner focus on Petitioner’s second argument, i.e., that the “firewall and intrusion protection options” of limitation 1.g are not described in the Provisional. *See, e.g.*, PO Resp. 24–25 (citing Ex. 2005 ¶ 32; Ex. 2003, 26, 34) (arguing the Provisional does not describe “patching” but rather “how the disclosed AVT system drops packets at the Snort Sensor, which is ‘an intrusion prevention system based occurrence mitigation type’”). The “user option” of limitation 1.g’s first appearance is at the filing of the preliminary amendment. *See* Ex. 1007, 555–556.

Patent Owner does not address whether the subject matter of the challenged claims, including limitation 1.g, is described in the ’852 application or its continuation child, the ’014 application.¹⁶ Patent Owner has the burden of production to produce evidence and supporting argument

¹⁶ At the oral hearing, Patent Owner argued that the ’237 application, that issued as the ’644 patent, is a continuation in part of the ’852 application only “for purposes of adding a glossary.” *See* Tr. 34:7–9. However, the record does not support Patent Owner’s assertion. For example, the ’852 application includes five drawing figures while the ’237 application for the ’644 patent includes thirteen drawing figures. Ex. 1009, 534–538; Ex. 1007, 657–668. The written description of the ’237 application and the ’852 application also differ. *Compare* Ex. 1007, 605 (“Field of the Invention” and “Summary”), *with* Ex. 1009, 516 (“Field of the Invention” and “Summary of the Invention”).

that the '644 patent is entitled to the priority of the previously filed applications, including the '852 application. *Dynamic Drinkware*, 800 F.3d at 1379; *see also* Inst. Dec. 11 (citing *Dynamic Drinkware*). Patent Owner acknowledges that it has the burden of production on the priority issue. *See* PO Resp. 22–23.

Petitioner affirmatively contends limitation 1.g is not disclosed in the '852 application. Pet. 31–32. Petitioner argues the '852 application explains, among other things, that “[b]ased on a prioritization previously selected by an administrator or the system designer, the remediation technique(s) are applied.” *Id.* at 31 (citing Ex. 1009, 704). The '852 application also explains that “[i]f a means of remediation of the vulnerability is known, the remediation can be selectively applied to only those devices subject to the vulnerability.” *Id.* (citing Ex. 1009, 705).

Relying on the preceding disclosures and the Nielsen Declaration, Petitioner concludes that “the only user selection disclosed appears to be a priority of the machines that are to be remediated.” *Id.* (citing Ex. 1011 ¶ 71). Petitioner contrasts the preceding disclosures with the November 12, 2014, preliminary amendment to the '237 application, which provides a “user option.” *Id.* at 31–32.

We find several of the drawing figures from the '237 application are from the Provisional, while none of the drawings from the Provisional are in the '852 application. *Compare* Ex. 1007, 663 (Fig. 7), *with* Ex. 1008, 34; Ex. 2003, 27. Patent Owner acknowledges that incorporation by reference is not available to satisfy section 120. *See* PO Sur-Reply 1–3. Absent incorporation by reference, the '852 application lacks much of what is disclosed in the Provisional and the '852 application breaks the continuity

required in order to comply with the written description requirement section 112. *See Lockwood*, 107 F.3d at 1571. We find that Patent Owner has not met its burden of production with respect to the '852 application and Petitioner has shown sufficiently that the '852 application does not reasonably convey to a person of ordinary skill that the inventor possessed the claimed subject matter of limitation 1.g.

Patent Owner did not respond in its papers or at oral hearing to Petitioner's argument that the subject matter of limitation 1.g does not appear in any of the previously filed applications until the preliminary amendment to the '237 application for the '644 patent was filed on November 12, 2014. *See* Pet. 30–32 (citing Ex. 1007, 556–557). The issue of the preliminary amendment was discussed by the Board during Petitioner's argument at the oral hearing. Tr. 23:13–24. Petitioner argues, in the context of the specification of the '644 patent, that there is no support for claim limitation 1.g. *Id.* at 24:1–28:16. The unrebutted testimony of Petitioner's expert, Dr. Nielson, is that the subject matter added by the preliminary amendment is not described in the Provisional. Ex. 1011 ¶ 69.

We find the preliminary amendment is the first time that any of the applications in the Chain of Applications (see table above) “*clearly allow* persons of ordinary skill in the art to recognize that [the inventor] invented what is claimed.” *Ariad*, 598 F.3d at 1351 (emphasis added) (citing *Vas–Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563 (Fed. Cir. 1991)). Only as of the filing of the preliminary amendment do any of the applications “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter.” *See id.* (citations omitted). Not

until the preliminary amendment was filed was it *clear* that the inventor possessed the claimed subject matter.

Having determined that the “user option” description for limitation 1.g was lacking in the Provisional, we need not address whether the “firewall and intrusion protection options” of limitation 1.g are described in the Provisional. Lack of written description for one claim is fatal for that claim. *See, e.g., Application of Borkowski*, 422 F.2d 904, 909 n.4 (C.C.P.A. 1970) (“A disclosure may, of course, be insufficient to support one claim but sufficient to support another.”). We find Petitioner has shown by a preponderance of the evidence that the Provisional does not reasonably convey to a person of ordinary skill that the inventor possessed the claimed subject matter of limitation 1.g as of the filing date of the Provisional.

In summary, “[i]n order to gain the benefit of the filing date of an earlier application under 35 U.S.C. § 120, each application in the chain leading back to the earlier application must comply with the written description requirement of 35 U.S.C. § 112.” *Lockwood*, 107 F.3d at 1571 (citing *In re Hogan*, 559 F.2d 595, 609 (CCPA 1977)). Neither the Provisional nor the ’852 application satisfies the written description requirement with respect to limitation 1.g, and Patent Owner has not met its burden of production with respect to claiming priority to a previously filed application under section 120. The effective filing date of the application for the ’644 patent is September 28, 2014, which is after the effective date of the AIA.

4. *Pre-AIA First to Invent*

Patent Owner argues that, under pre-AIA law, it can prove a prior invention date. *See* PO Resp. 25–40. As discussed above, we have found

Patent Owner is not entitled to a filing date that would require this proceeding to be decided under the first to invent pre-AIA law. Patent Owner acknowledges that its evidence of prior invention is not relevant if it is not entitled to the asserted earlier priority date. Tr. 70:4–9. We need not decide the first-to-invent argument or its supporting evidence as presented by Patent Owner.

B. Claim Construction

In this *inter partes* review, claim terms are given their broadest reasonable interpretation in light of the specification in which they appear. See 37 C.F.R. § 42.100(b) (2017).¹⁷ We construed six terms in the Institution Decision. Inst. Dec. 11–19. Post institution, neither party has any objections to our preliminary claim construction. See Tr. 29:2–13 (Petitioner); PO Resp. 14 (repeating constructions from Institution Decision); Tr. 51:3–9 (Patent Owner). None of the construed terms resolve any dispute raised. “[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” See *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Nonetheless, as we noted in the

¹⁷ The Office recently changed the claim construction standard applicable to an *inter partes* review. See Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018). The rule changing the claim construction standard, however, does not apply to this proceeding because Petitioner filed its Petition before the effective date of the final rule, i.e., November 13, 2018. *Id.* at 51,340 (rule effective date and applicability date), 51,344 (explaining how the Office will implement the rule).

Institution Decision, independent claim 1 includes terms not discussed in the specification and uses complex syntax, and construction of some terms “will aid in parsing the claim.” Inst. Dec. 12. Our preliminary constructions are set out below as final constructions, for the reasons we have stated in our Institution Decision.

1. “*actual vulnerability information*”

The first limitation of claim 1, limitation 1.b, recites

code for receiving *actual vulnerability information* from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including

Pet. 34; Ex. 1001, 31:25–29.

The broadest reasonable interpretation of “actual vulnerability information” is “information about actual vulnerabilities of a device generated based on potential vulnerability information.” See Inst. Dec. 13–14.

2. “*occurrence*”

Limitation 1.e recites “code for identifying an *occurrence* in connection with at least one of the plurality of devices.” Pet. 37; Ex. 1001, 31:43–44. The broadest reasonable interpretation of “occurrence” is “an event that seeks to take advantage of a vulnerability.” See Inst. Dec. 14–15.

3. “*selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types*”

Part of limitation 1.g recites “selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types.” Pet. 39; Ex. 1001, 31:52–53. The broadest reasonable interpretation of this term is “selecting for use one or more actions of different types that mitigate

exploitation of the vulnerability.” *See* Inst. Dec. 15–16.

4. *“including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type”*

Another part of limitation 1.g recites “including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type.” Pet. 39; Ex. 1001, 31:54–56. The broadest reasonable interpretation of this term is “an occurrence mitigation action performed by generic firewall technology (such as blocking an attempted connection) and/or a generic intrusion prevention system technology (such as dropping an existing connection).” *See* Inst. Dec. 16–17.

5. *“utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices”*

Another part of limitation 1.g recites “utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.” Pet. 39; Ex. 1001, 31:58–60. The broadest reasonable interpretation of this term is “at least one of the devices of a plurality of devices is capable of using at least two different ‘occurrence mitigation actions.’” *See* Inst. Dec. 17–18.

6. *“an intrusion prevention system-based occurrence mitigation . . . for occurrence mitigation by preventing advantage being taken of actual vulnerabilities”*

Another part of limitation 1.g recites “an intrusion prevention system-based occurrence mitigation . . . for occurrence mitigation by preventing advantage being taken of actual vulnerabilities.” Ex. 1001, 31:54–58. The broadest reasonable interpretation of this term is “an intrusion prevention system that mitigates actual vulnerabilities.” *See* Inst. Dec. 18–19.

C. Claim 1 as Anticipated by Shah (Ground 1)

Petitioner argues claim 1 is anticipated under §102(a)(1) by Shah. Pet. 32–40. Above, we determined that Shah was prior art to the '644 patent. See Section III.A. Petitioner's argument is supported by the Nielsen Declaration. Ex. 1011 ¶¶ 90–129.

1. Overview of Shah (Ex. 1002)

Shah discloses

[a]n intrusion detection method wherein a vulnerability determination or vulnerability assessment of one or more computers or hosts is performed to determine whether and what vulnerabilities exist on the computers or hosts, accomplished by using existing vulnerability determination or vulnerability assessment information that can be continually updated. Attack signatures, which can also be continually updated, are identified and correlated with the specific vulnerabilities identified. One or more designated IP sessions associated with attempted vulnerability exploitation are then inhibited or disconnected.

Ex. 1002, Abstract. Shah's system "can interact with the security system's firewall, and can provide a highly effective response that can either disconnect (or block) malicious communication traffic or connections, or instruct a firewall to do so, without disrupting legitimate traffic." *Id.* ¶ 19.

In one embodiment, Shah discloses a separate computer as an adaptive intrusion detection system. Ex. 1002 ¶ 21. Figure 1 of Shah is reproduced below.

FIG. 1

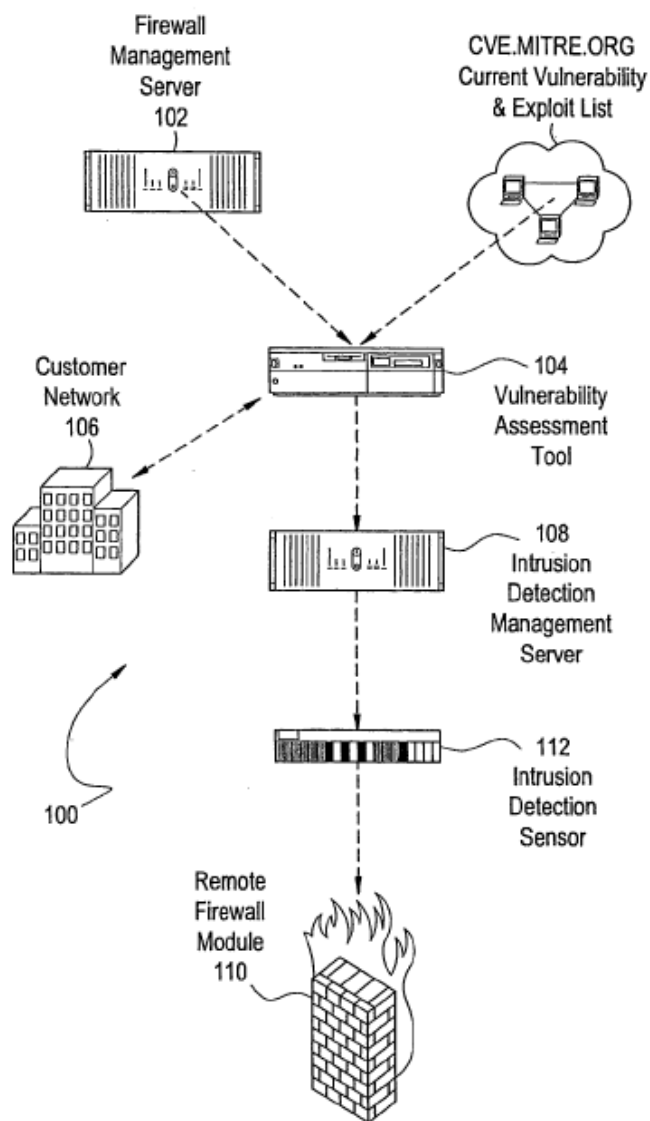


Figure 1 illustrates the adaptive intrusion detection system 100. *Id.* As shown in Figure 1, “firewall policy information is transferred from the firewall management server 102 into a vulnerability assessment or determination tool 104.” *Id.* A currently updated list of vulnerabilities, shown as CVE.MITRE.ORG, “Current Vulnerability & Exploit List” in Figure 1, is then also loaded into vulnerability assessment or determination tool 104. *Id.* This list may be stored on firewall management server 102,

stored on a separate hardware device, or stored at a separate location. *Id.*

“Based upon the information contained in the fire wall policy and the vulnerabilities list” the “vulnerability assessment tool 104 conducts an attack” on one or more computers or hosts of the “computer network 106 that had been designated as potentially vulnerable to attack.” Ex. 1002 ¶ 22. The vulnerabilities of the computer network are determined and those vulnerabilities loaded onto intrusion detection management server 108, which correlates vulnerabilities with identifiable attack signatures. *Id.* “The intrusion detection management server 108 is then preferably instructed to only identify these attack signatures” and “instructs a firewall 110 to block the specific sessions that have been identified.” *Id.*

2. *Discussion—Anticipation by Shah (claim 1)*

In the Institution Decision we initially declined to include the anticipation ground in the trial because “Petitioner’s use of different embodiments from Shah to meet all the claim limitations” precluded that reference from anticipating claim 1. Inst. Dec. 23 (citing *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (internal citations omitted)). SAS required the inclusion of anticipation by Shah as a ground in the trial. See Mod. Inst. Dec.

The challenge based on anticipation by Shah was withdrawn at oral hearing. Petitioner stated “I’m not going to contest that claim for anticipation.” Tr. 29:14–19. Accordingly, Petitioner has abandoned the contest on the challenge based on anticipation by Shah. 37 C.F.R. § 42.73(b)(4).

D. Asserted Obviousness Grounds

Petitioner asserts claim 1 would have been obvious over Shah and Hill. Pet. 40. Petitioner also asserts claims 1, 7, and 14 would have been obvious over Gupta and Girouard and also over Gleichauf and Hill. *Id.* at 46, 62.

1. Law of Obviousness

A patent claim is invalid as obvious if the differences between the claimed subject matter 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.” 35 U.S.C. § 103(a).

“The ultimate determination of obviousness is a question of law, but that determination is based on underlying factual findings The underlying factual findings include (1) ‘the scope and content of the prior art,’ (2) ‘differences between the prior art and the claims at issue,’ (3) ‘the level of ordinary skill in the pertinent art,’ and (4) the presence of secondary considerations of nonobviousness such ‘as commercial success, long felt but unsolved needs, failure of others,’ and unexpected results.” *Nuvasive*, 842 F.3d at 1381 (quoting *inter alia* *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)).

In assessing the prior art, the Board must consider whether a person of ordinary skill would have been motivated to combine the prior art to achieve the claimed invention. *Nuvasive*, 842 F.3d at 1381. As the Federal Circuit found, in quoting from the Supreme Court’s decision in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007),

because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of

necessity will be combinations of what, in some sense, is already known,” “it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does.

Personal Web Techs., LLC v. Apple, Inc., 848 F.3d 987, 991–992 (Fed. Cir. 2017) (quoting *KSR*, 550 U.S. at 418–19).

2. *Person of Ordinary Skill in the Art*

Petitioner asserts that a person having ordinary skill in the art would have a B.S. degree in Computer Science or equivalent. Pet. 20 (citing Ex. 1011 ¶¶ 55–56). Dr. Nielson’s testimony is that a person of ordinary skill would have a B.S. in Computer Science “*plus* one-to-two years of experience” in network administration. Ex. 1011 ¶¶ 55–56. Dr. Nelson also testifies additional education without experience, or more experience, would also describe a person of ordinary skill. Petitioner’s proposal as augmented by the Nielson Declaration was adopted for purposes of the Institution Decision. Inst. Dec. 26.

Patent Owner’s expert opines that a person of ordinary skill would have either a Master’s Degree in Electrical Engineering or an undergraduate degree in Electrical Engineering or related discipline and “two years of relevant work experience in industry.” Ex. 2005 ¶ 23. We find that the two descriptions are substantially the same and there is no material dispute as to the level of ordinary skill. We maintain the description from the Institution Decision as follows:

a person having ordinary skill in the art would have a B.S. degree in Computer Science or equivalent. See Pet. 20 (citing Ex. 1001 ¶¶ 55–56). Dr. Nielson’s testimony is a B.S. in Computer Science “*plus* one-to-two years of experience” in network administration. Ex. 1011

¶¶ 55–56). Dr. Nelson also testifies additional education without experience or more experience would also describe a person of ordinary skill.

3. Claim 1 as Obvious Over Shah and Hill (Ground 2)

Petitioner argues claim 1 would have been obvious under section 103 over Shah and Hill. Pet. 40–46. Petitioner’s argument is supported by the Nielson Declaration. Ex. 1011 ¶¶ 130–150. Patent Owner again asserts that Shah is not prior art. PO Resp. 41. We rejected that argument above. See Section III.A. Patent Owner further argues the combination of Shah and Hill does not show certain limitations of claim 1. PO Resp. 41–47. For reasons detailed below, we agree with Petitioner.

a. Overview of Shah (Ex. 1002)

An overview of Shah is found in Section III.C.1 above.

b. Overview of Hill (Ex. 1003)

Hill teaches “[a] dynamic network security system (20) responds to a security attack (92) on a computer network (22) having a multiplicity of computer nodes (24).” Ex. 1003, Abstract. “Security events” are “received from the security agents (36) to form an attack signature (94) of the attack (92).” *Id.* Multidimensional attack status information and recommended actions for mitigating the attack are displayed. *Id.*

Specifically, Hill teaches a network status display which includes an attack signature log that “provides current and historical perspective on a given attack record at various sample times.” Ex. 1003, 8:62–9:2. The display includes an attack mitigation list cataloging actions to mitigate a “first attack.” Ex. 1003, 9:4–7.

c. Analysis—Obviousness of Claim 1 Over Shah and Hill

Petitioner’s showing is discussed below on a limitation-by-limitation basis. We address Patent Owner’s arguments with respect to those limitations it disputes.

Petitioner asserts a person of ordinary skill “would have been motivated to combine the teachings of Shah and Hill because Shah describes identifying network attacks and Hill describes presenting information related to identified network attacks.” Pet. 41. Further, Petitioner contends a person of ordinary skill would have been motivated to use the methods of Hill to present information about identified network attacks to allow a network operator to understand the nature of the network attack Shah identifies. *Id.* (citing Ex. 1011 ¶ 136). Finally, Petitioner contends “[a]ll claim limitations were known in Shah and Hill and a PHOSITA would have combined the teachings of these known methods with no change in their respective functions, and the combination would have yielded nothing more than predictable results to a PHOSITA.” *Id.* (citing *KSR*, 550 U.S. at 416).

Patent Owner argues generally “the Petitioner did not show that a ‘skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” PO Resp. 2 (quoting *OSRAM Sylvania, Inc. v. Am. Induction Techs., Inc.*, 701 F.3d 698, 706 (Fed. Cir. 2012)). Patent Owner makes no specific argument regarding the Shah and Hill combination nor does Patent Owner present an argument specific to any other ground asserted by Petitioner. *See id.* at 2–3. Patent Owner does not cite, and we are not aware of, any precedential authority going so far as to say “objective evidence” like

experimental data is required to support the reason to combine the references. *See id.*

We find Petitioner’s argument and evidence of motivation, based on Hill allowing a network operator to understand the nature of the network attack Shah identifies, are sufficient to demonstrate a motivation for a person of ordinary skill to have combined Hill with Shah. We also find that both Shah and Hill separately teach all of the claim limitations, and combining them would lead to a predictable result of identifying attack threats and responding to them, a result that *both* references teach. “Although predictability is a touchstone of obviousness, the ‘predictable result’ discussed in *KSR* refers not only to the expectation that prior art elements are capable of being physically combined, but also that the combination would have worked for its intended purpose.” *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1365 (Fed. Cir. 2016) (quoting *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1326 (Fed. Cir. 2009)). We find that the argument and evidence of a predictable result show the “combination would have worked for its intended purpose” and the combination would have had a reasonable expectation of success along with the motivation to make the combination.

Limitation 1.a, the preamble of claim 1, recites “[a] computer program product embodied on a non-transitory computer readable medium.”¹⁸ As

¹⁸ As we did in the Institution Decision, we find the preamble is entitled to patentable weight because “computer program product” gives a context for the term “code for” recited in limitations following the preamble. Inst. Dec. 27 n.10 (citing *In re Paulsen*, 30 F.3d 1475, 1479 (Fed. Cir. 1994) (“computer” appearing only in the preamble “breathes life and meaning into the claims and, hence, is a necessary limitation to them”)).

Petitioner argues, we find that Shah teaches a computer program product. *See* Pet. 42 (citing Ex. 1002 ¶ 32; Ex. 1011 ¶ 138). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.a.

Limitation 1.b recites, in pertinent part, “code for receiving actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities.” We find that Shah’s vulnerability assessment tool determines “actual vulnerability information.” *See* Pet. 42 (citing Ex. 1002 ¶¶ 21–23, Fig. 1). Shah also teaches an embodiment¹⁹ where the intrusion detection system is on a separate computer and a central computer, transfers “Vulnerability information and Assessment (VA)” files to its local operating system. *Id.* at 25 (citing Ex. 1002 ¶ 25, Fig. 21 [2]). We find that Petitioner’s citation to Shah’s paragraph 25 and Figure 1 shows “regularly updating potential vulnerability information from a second data storage.” *Id.* (citing Ex. 1011 ¶ 139). Based on the cited argument and evidence, including Shah’s vulnerability assessment tool, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.b.

Limitation 1.c recites “at least one first potential vulnerability, and at least one second potential vulnerability.” Petitioner argues “Shah discloses a

¹⁹ Unlike in its challenge based on anticipation, when asserting obviousness, Petitioner may rely on different embodiments of the same prior art reference. *See Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009) (combining two separate embodiments from the same reference “does not require a leap of inventiveness”).

‘Current Vulnerability & Exploit List’ containing potential vulnerability information for a plurality of potential vulnerabilities.” Pet. 43 (citing Ex. 1002 ¶ 21, Fig. 1; Ex. 1011 ¶ 140). Based on the cited evidence, including Shah’s “Current Vulnerability & Exploit List” and the Nielson Declaration, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.c.

Limitation 1.d recites

said actual vulnerability information generated utilizing the potential vulnerability information, in response to code execution by at least one processor, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities.

Petitioner cross references its arguments that Shah anticipates limitation 1.d. See Pet. 43 (citing Ex. 1011 ¶ 141). Petitioner’s anticipation evidence, including the Nielson Declaration, supports its showing that Shah teaches limitation 1.d. See *id.* at 36–37 (citing Ex. 1002 ¶¶ 21–23, 26, Fig. 1; Ex. 1011 ¶¶ 107, 114). Petitioner cites to the same citations from Shah in its obviousness challenge, which Petitioner argues “disclose[s] identifying specific devices and services offered by those devices,”²⁰ thus

²⁰ The evidence of record also includes the assertion that “[t]he skilled artisan would also understand that many embodiments of ‘systems and services’ described would include at least three devices.” See Pet. Reply 16 (citing *inter alia* Ex. 1011 ¶ 109; see also *id.* (citing Ex. 1002 ¶ 26 (“The intrusion detection system, through utilization of an interface such as an application interface (API), securely queries a repository . . . for Internet Protocol (IP) addresses and services which are offered by computers or

identifying at least one configuration associated with a plurality of devices.”
Pet. 43 (citing Ex. 1002 ¶¶ 21–23, 26, Fig. 1; Ex. 1011 ¶¶ 107, 114).

In connection with limitation 1.d, Petitioner cites to paragraph 21 of Shah. *Id.* at 36–37, 43. Paragraph 21 of Shah teaches “firewall policy information is transferred”²¹ from a server to the “vulnerability assessment or determination tool 104.” Paragraph 21 of Shah then teaches creating a list of vulnerabilities which are also loaded onto the “determination tool 104” and stored on a server. The list of vulnerabilities are “actual vulnerabilities” identified from potential vulnerabilities identified as per the firewall policy. Shah thus teaches “actual vulnerability information generated utilizing the potential vulnerability information” as we have construed the term.” *See* Section III.C.1 above.

Petitioner’s incorporated anticipation arguments quote from Shah as teaching “[t]he vulnerabilities of this equipment and its resident systems and services are then determined and preferably loaded onto an intrusion detection management server 108.” Pet. 36 (quoting Ex. 1002 ¶ 22), 43. Paragraph 22 of Shah further teaches that the management server 108 “correlates these vulnerabilities with attack signatures” and is preferably instructed to “only identify these attack signatures.” Ex. 1002 ¶ 22.

Patent Owner disputes Petitioner’s showing and breaks limitation 1.d into limitation limitations 1.4 and 1.5. PO Resp. 44–45. Limitation 1.4 recites “identifying at least one configuration associated with a plurality of

hosts, protected by the security gateway, to the public Internet.”)).

²¹ The firewall “can either disconnect (or block) malicious communication traffic or connections, or instruct a firewall to do so, without disrupting legitimate traffic.” Ex. 1002 ¶ 19.

devices including a first device, a second device, and a third device.” *Id.* at 44. Patent Owner argues Shah uses attack signatures of known vulnerabilities and determines if “actual attacks” are occurring by correlating the attack signatures with the attack signatures of the known vulnerabilities. *Id.* at 42 (citing Ex. 1002, Abstract, ¶ 22). Patent Owner asserts this procedure is part of Shah’s intrusion detection sensor, which detects intrusions and then uses a firewall to “prevent packets from reaching a vulnerable destination.” *Id.* at 42–43 (citing Ex. 1002, Fig. 1 (annotated with the sensor in a green block and the firewall in a red block)); *see also* Ex. 2005 ¶¶ 47–50 (neither Shah nor Hill disclose limitation 1.d/1.4).²²

Patent Owner argues specifically that Shah’s vulnerability assessment tool’s function is to “conduct[] an attack on the relevant equipment on computer network 106 that had been designated as potentially vulnerable to attack.” PO Resp. 22 (citing Ex. 1002 ¶ 22). Patent Owner concludes Shah does not teach the recited “identifying at least one configuration associated with a plurality of devices.” *Id.* at 44–45 (citing Ex. 1002 ¶¶ 22, 24; Ex. 2005 ¶ 53).

We are not persuaded by Patent Owner’s argument. Petitioner shows that Shah discloses “vulnerabilities of this equipment and its resident systems and services are . . . determined” and “correlate[d] [with] attack signatures.” Pet. 36 (citing Ex. 1002 ¶ 21). Petitioner responds in its Reply that Shah teaches “that an interface such as an application interface (API), securely queries a repository located within a security gateway, or a

²² According to Patent Owner, Hill also “uses simulated attacks to determine potential vulnerabilities.” PO Resp. 43 (citing Ex. 1003, 2:66–3:16, Figs. 1, 2; Ex. 2005 ¶ 48). Petitioner relies on Shah alone to teach limitation 1.d.

management station, for **Internet Protocol (IP) addresses and services which are offered by computers or hosts.**” Pet. Reply 15 (citing Ex. 1002 ¶ 26). The Nielson Declaration testimony is that a person of ordinary skill “would have understood that configuration information was identified to determine IP addresses, resident systems, and services associated with the devices.” *Id.* (citing Ex. 1002 ¶¶ 22, 26–27; Ex. 1011 ¶ 109).

We have reviewed paragraph 53 of the cited testimony from the Feamster Declaration regarding device configuration. Paragraph 53 is worded identically to Patent Owner’s Response. *See* PO Resp. 44–45; Ex. 2005 ¶ 53. Patent Owner’s Sur-Reply does not respond to the contention in Petitioner’s Reply that device configuration information is identified in order to determine “IP addresses, resident systems and services associated with the devices.” Neither did Dr. Feamster submit a responsive declaration disputing the testimony of Dr. Nielson. We credit Dr. Nielson’s testimony and are persuaded that Shah teaches making a vulnerability determination based on device configuration. *See* Ex. 1011 ¶ 109 (“[C]onfiguration information is used in determining systems and services present in the network.”), *see also id.* ¶ 108 (“[C]onfiguration information is used in determining systems and services present in the network.”).

Limitation 1.5 is Patent Owner’s second designation for Petitioner’s limitation 1.d. PO Resp. 45. Limitation 1.5 recites “determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities.” *Id.* Patent Owner contends Petitioner’s citations to Shah at pages 36 and 37 of the Petition are “isolated” and do not teach the recited

claim language. *Id.* (citing Ex. 1002 ¶¶ 21–23, 26, Fig. 1). Patent Owner contends the showing has no “supporting analysis or explanation.” *Id.* (citing Ex. 2005 ¶ 56).

We are persuaded that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.5. Above, we discussed Petitioner’s showing regarding Shah’s generation of actual vulnerability information for system devices based on utilizing potential vulnerability information contained in the firewall policy and vulnerabilities list. Petitioner notes that page 36 of the “Petition quotes Shah for this element.” Pet. Reply 16. The quote from Shah is “[t]he vulnerabilities of this equipment and **its resident systems and services** are then determined.” *Id.* (quoting Ex. 1002 ¶ 22) (emphasis by Petitioner). Petitioner also cites to the Nielson Declaration. *Id.* (citing Ex. 1011 ¶¶ 107–110). In addition to what is taught by Shah, we credit the Nielson Declaration opinion testimony that Shah discloses “determining that the plurality of devices is actually vulnerable to at least one actual vulnerability.” Ex. 1011 ¶ 110 (citing Ex. 1002 ¶ 22), *see also id.* ¶ 108 (“Shah’s claim 16 reads in part: retrieving network and system **configuration information**; retrieving vulnerability information and attack signature rules.”). Patent Owner does not dispute this testimony or provide any evidence to the contrary. Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation(s) 1.d/1.4 and 1.5.

Limitation 1.e/1.6 recites “code for identifying an occurrence in connection with at least one of the plurality of devices.” Petitioner argues “Shah discloses detecting attacks directed at vulnerable devices, thus identifying an occurrence in connection with at least one the plurality of

devices.” Pet. 44 (citing Ex. 1002 ¶ 29; Ex. 1011 ¶ 142). The Nielson Declaration is relied on as evidence that a person of ordinary skill “would understand a detected attack as an ‘occurrence.’” *Id.* (citing Ex. 1011 ¶ 115).

Patent Owner disputes Petitioner’s showing regarding limitation 1.e/1.6. PO Resp. 45–46. Patent Owner acknowledges an *actual* attack can be an occurrence but argues that Shah discloses only a *simulated* attack. *Id.* at 46 (citing Ex. 2005 ¶ 59). Citing our construction of “occurrence” as “an event that seeks to take advantage of a vulnerability,” Patent Owner seems to argue Shah does not identify an “occurrence” because a simulation cannot be an actual event. *Id.*

Patent Owner’s argument is not persuasive. The citation to the testimony from the Feamster Declaration is a copy of the Response. See PO Resp. 46; Ex. 2005 ¶ 59. The Feamster Declaration Opinion is based solely on the contention that Shah uses “simulated” attacks. Ex. 2005 ¶ 59. Shah describes attacking devices with known vulnerabilities in order to perform a vulnerability assessment of any given piece of equipment. Ex. 1002 ¶ 21. Shah then lists vulnerabilities and loads them into the vulnerability assessment or determination tool. *Id.* ¶ 22. Finally, Shah correlates vulnerabilities with attack signatures and blocks the traffic that matches an attack signature. *Id.*; see also Pet. Reply 18 (citing Ex. 1002 ¶ 29 (“Armed with the attack signatures the detection engine can identify specific traffic that is destined for a computer with a specific software defect.”); see also Ex. 1011 ¶¶ 115–117 (Nielson Declaration relying on Shah paragraphs 29, 31, and 32 to conclude in paragraph 117 that Shah would “enable one of

skill in the art” to “practice this limitation”²³). In other words, Shah blocks traffic that seeks to attack a vulnerability of a piece of equipment. That the attack is stopped, in part, by a database created by “simulated” attacks does not make the attack any less real of an event. Based on the cited argument and evidence, including the Nielson Declaration, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.e/1.6.

Limitation 1.f/1.7 recites “code for determining that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the actual vulnerability information.” Petitioner argues that “Shah discloses identifying specific traffic based on tailored attack signatures, thus determining that an actual vulnerability is susceptible to exploitation by an occurrence.” Pet. 44 (citing Ex. 1002 ¶¶ 29–30; Ex. 1011 ¶ 118).

Patent Owner disputes Petitioner’s showing regarding limitation 1.f/1.7. PO Resp. 46–47. Patent Owner argues “Shah never disclosed determining any actual vulnerability based on a device’s configuration.” *Id.* at 47 (citing Ex. 2005 ¶ 62). As we already found, Shah does identify device configuration by, for example, IP address. *See above* re limitation 1.d/1.4. We agree with Petitioner that “Shah discloses identifying at least one configuration, determining actual vulnerabilities based on the identified configuration, and determining that an actual vulnerability is susceptible to

²³ We understand that Dr. Neilson’s testimony to be that Shah teaches the limitation as a factual matter, rather than being an opinion on the legal question of whether Shah is enabling.

an occurrence.” Pet. Reply 20 (citing Pet. 38, 44; Ex. 1011 ¶¶ 121, 118, 143). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Shah teaches limitation 1.f/1.7.

Limitation 1.g recites

code for providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.

Petitioner applies its construction, which we have adopted for purposes of this Decision, that a “firewall based mitigation type” includes “generic firewall technology (such as blocking an attempted connection).” Pet. 45. Petitioner also construes “intrusion prevention system based occurrence mitigation type” as including “any occurrence mitigation action that may be performed by generic intrusion prevention system technology (such as dropping an existing connection).” *Id.*; *see also* Section III.C.6 above (construing “intrusion prevention system” limitation).

Petitioner cites the arguments it made in connection with anticipation by Shah relative to limitation 1.g. Pet. 45; *see also id.* at 39–40 (anticipation showing on limitation 1.g). Shah specifically teaches “mitigation technique options” including “updated information databases, firewall policy configurations, and the intrusion detection logs.” *Id.* at 39 (citing Ex. 1002 ¶ 20; Ex. 1011 ¶ 122).

Relying on Hill and the Nielson Declaration, Petitioner argues Hill discloses “an occurrence mitigation action performed by a firewall.” Pet. 45–46 (citing Ex. 1003, 8:50–55; Ex. 1011 ¶ 146). Further relying on Hill and the Nielson Declaration, Petitioner argues “Hill also discloses providing false, but realistic data, which a [person of ordinary skill in the art] would understand to be an occurrence mitigation action performed by an intrusion prevention system.” *Id.* at 45–46 (citing Ex. 1003, 9:4–7; Ex. 1011 ¶ 146).

Petitioner has shown by a preponderance of the evidence that Shah or Shah in view of Hill teaches limitation 1.g. Both references are cited for every recitation of limitation 1.g. See Pet. 45 (citing both Shah and Hill). We understand Petitioner to be arguing that Shah alone or, in the alternative, Shah in view of Hill teaches limitation 1.g. See Pet. 46 (citing Ex. 1011 ¶ 148).

d. Summary of Obviousness Over Shah and Hill

Petitioner’s argument and supporting evidence have shown by a preponderance of the evidence that the subject matter of claim 1 would have been obvious over Shah and Hill.

4. Claims 1, 7, and 14 as Obvious Over Gupta and Girouard (Ground 3)

Petitioner argues claims 1, 7, and 14 would have been obvious under § 103 over Gupta and Girouard. Pet. 46–61. Petitioner’s argument is supported by the Nielson Declaration. Ex. 1011 ¶¶ 151–225. Patent Owner again asserts that Girouard is not prior art. PO Resp. 47. We rejected that argument above. See Section III.A. Patent Owner further argues the combination of Gupta and Girouard does not show certain limitations of claims 1, 7, and 14. PO Resp. 47–60. For reasons detailed below, we agree with Petitioner.

a. Overview of Gupta (Ex. 1004)

Gupta describes “[a] method of provisioning a computer against computer attacks includes constructing a hierarchy characterizing different computer attacks and counter measures, and traversing this hierarchy to identify computer attacks and countermeasures relevant to a target platform.” Ex. 1004, Abstract. Detection and protection measures are collected and “protection measures are then downloaded to a security sensor associated with the target platform.” *Id.*

The collected detection and protection measures “can result in an attack file.” Ex. 1004 ¶ 164. A sensor with protective software is downloaded for the target platform. *Id.* “The hierarchical approach of the invention allows one to clearly describe, in one data structure, what attacks a given environment is vulnerable to, what protection means (mechanisms and signatures) are available, and how detection alerts are correlated.” *Id.* ¶ 165. In sum, Gupta teaches a security system that identifies computer attacks with reference to specific devices, lists a hierarchy characterizing different computer attacks, and determines appropriate counter measures against the attacks.

b. Overview of Girouard (Ex. 1005)

Girouard teaches a threat database containing a “compilation of one or more vulnerabilities that have been received.” Ex. 1005 ¶ 41. Girouard further describes a vulnerability manager may “relate a threat database to a configuration database of computer systems” which “may generate a list of vulnerable systems.” *Id.* ¶ 59. The vulnerability management system “may perform corrective action” in response to a work order, including downloading a patch. *Id.* ¶ 60. Among other things, the vulnerability

manager 154 may generate a display “with the resources required to perform the corrective action.” *Id.* ¶ 61.

c. Analysis - Obviousness of Claims 1, 7, and 14 over Gupta and Girouard

Petitioner asserts a person of ordinary skill would have been motivated to combine Gupta and Girouard because “Gupta describes approaches to identifying vulnerabilities and Girouard describes corrective actions to identified vulnerabilities.” Pet. 47 (citing Ex. 1011 ¶ 158); *see also id.* at 58 (a person of ordinary skill “would have recognized the benefit of combining Girouard’s additional mitigation techniques, such as a firewall, with Gupta’s provision of multiple mitigation options”); *see also* Ex. 1011 ¶¶ 224–225 (claim 1 obvious over Gupta and Girouard). Petitioner argues a person of ordinary skill would be motivated to combine Girouard’s options to take corrective action with Gupta’s security system that identifies vulnerabilities on specific devices. The known corrective actions of Girouard with the Gupta’s method of identifying vulnerabilities would result in “the predictable outcome of identifying and implementing corrective action for the identified vulnerabilities.” *Id.* at 48 (citing *KSR*, 550 U.S. at 416–417).

Patent Owner makes the same general argument regarding motivation and reasonable expectation of success that we found unpersuasive in Section III.D.3.c above. For the reasons stated above, we find Petitioner has shown, by preponderance of the evidence, a motive to combine Gupta and Girouard, and reasonable expectation of success in identifying and implementing corrective action for the identified vulnerabilities from doing so. As we discuss below, Petitioner has also shown, by a preponderance of the

evidence, that Gupta and/or Girouard teaches each of the limitations of claim 1.

(1) Claim 1

Petitioner cites to Gupta as teaching the preamble, limitation 1.a.²⁴ Pet. 48. Petitioner argues Gupta teaches a memory or alternatively a processor for storing and executing programs. *Id.* (citing Ex. 1004 ¶ 37). Based on the cited argument and evidence, we find that Petitioner has shown that Gupta teaches limitation 1.a.

Limitation 1.b recites, in pertinent part, “code for receiving actual vulnerability information from at least one first data storage” and “at least one second data storage that is used to identify a plurality of potential vulnerabilities.” Petitioner references its construction for “actual vulnerability information”²⁵ to argue that “Gupta discloses an ‘attack file’ that identifies ‘computer attacks and counter measures relevant to the target platform (block 162)’ and ‘clearly describe[s], in one data structure, what attacks a given environment is vulnerable to.’” Pet. 49 (quoting Ex. 1004 ¶¶ 164–165; Ex. 1011 ¶¶ 165, 167).

Patent Owner disputes that Petitioner has shown, or that the Neilson Declaration supports, a finding that Gupta teaches limitation 1.b. PO Resp. 48–51. Patent Owner argues

²⁴ Each limitation is set forth in full in Sections II.C and III.D.3 above.

²⁵ Petitioner proposed that “actual vulnerability information” means “information indicating that one or more devices are susceptible to threats that will take advantage of one or more vulnerabilities.” Pet. 21. We construed “actual vulnerability information” to mean “information about actual vulnerabilities of a device generated based on potential vulnerability information.” See Section III.B.1.

[t]he problem with Dr. Nielsen’s arguments at ¶¶ 165–173 is that the attack file is not generated after it passes through the hierarchical attack categorization module, and no further processing is described in Gupta. Thus, there cannot be a “*centralized attack file*” and a “*sensor-specific attack file*.” Gupta even describes the attack file using the exact same reference number —149—that indicates it is the exact same file in both of the portions of Gupta relied upon by Dr. Nielsen.

Id. at 50 (emphasis added) (citing Ex. 2005 ¶ 69). Ultimately, Patent Owner argues the attack file cannot be both the recited “first” and “second data storage.” *Id.* (citing Ex. 2005 ¶ 70). Patent Owner also asserts that “an attack file cannot be a data storage” as recited. Pet. 50 (citing Ex. 2005 ¶ 70).

Patent Owner breaks the Nielson Declaration into two parts, one for each recited data storage. For the first data storage, Patent Owner cites to that part of the Nielson Declaration that states “[t]here is an attack file maintained in the sensor management system that includes the potential vulnerability data.” PO Resp. 50; *see also* Ex. 1011 ¶ 167 (Dr. Nielson’s testimony). For the second data storage Patent Owner cites to the second part of the Nielson testimony that “there is a custom-crafted attack file derived with actual vulnerability information for a specific sensor to protect specific systems.” *Id.*

According to Patent Owner for the second data storage, the Nielson Declaration relies on the embodiment shown in Figure 15 of Gupta that “[t]he secure update download module 148 includes executable code to download an attack file 149 to a sensor management system 26.” PO Resp. 50–51 (quoting Ex. 1004 ¶ 168, Fig. 15); *see also* Ex. 1011 ¶ 166 (Dr. Nielson’s testimony re storage

for “potential vulnerability information”). For the first data storage, Patent Owner argues the Nielson Declaration cites to a portion of Gupta describing a different embodiment, taught in Figure 17 of Gupta and also described as “an attack file 149.” *Id.* at 51 (citing Ex. 1004 ¶ 169); *see also* Ex. 1011 ¶ 169 (Dr. Nielson’s testimony regarding storage for “actual vulnerability information”).

Patent Owner argues “[t]he same exact attack file 149” is referred to in both cited portions of Gupta. *Id.* Patent Owner concludes there cannot be two different attack files, as it argues Dr. Nielson testifies. *Id.* Patent Owner relies on the Feamster Declaration for support that the Nielson Declaration would require the attack file of Figure 15 to be different from the attack file of Figure 17. *Id.* (citing Ex. 2005 ¶ 71).

We are not persuaded that Gupta’s “attack files” are always the “exact same” file and that, as a result, Dr. Nielson’s testimony should be discounted. Patent Owner does not address testimony from the Nielson Declaration that “there are multiple version[] of the attack file” between the discussion in paragraphs 166 and 169 of second data storage and first data storage respectively. Ex. 1011 ¶ 167. Gupta supports this conclusion and makes clear that there may be different “attack files.” *See, e.g.*, Ex. 1004 ¶ 151 (referring to “code to download *an* attack *file*”), *id.* ¶ 152 (“deliver *updated* attack *files*”) (emphasis added).

Dr. Nielson’s testimony states that an “attack file” is downloaded to the “sensor management system” as part of the second data storage for “potential vulnerability information.” Ex. 1011

¶¶ 167–168. Dr. Nielson’s testimony also quotes from Gupta as teaching that a sensor, i.e., first data storage, receives potential vulnerability information from the second data storage and a “download, with the protective software (e.g., the attack file) for the target platform (block 166).” *Id.* ¶ 169 (citing Ex. 1004 ¶ 164, Fig. 17). Beyond the argument related to “attack files,” Patent Owner does not contest this evidence. *See* Pet. Reply 21–22 (citing PO Resp. 51). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Gupta teaches limitation 1.b.

Limitation 1.c recites in pertinent part, a “first” and a “second potential vulnerability.” Petitioner cites to Gupta’s teaching that “[t]he hierarchical attack categorization module 150 is used to develop, deploy and manage information on different computer attacks and countermeasures.” Pet. 51 (citing Ex. 1004 ¶ 154). Petitioner also cites the Nielson Declaration which concludes Gupta discloses this limitation. *Id.* (citing Ex. 1011 ¶ 174; *see also id.* ¶ 175 (quoting Ex. 1004 ¶¶ 155–159) (listing potential vulnerabilities)). Based on the cited argument and evidence, including Gupta’s hierarchical attack categorization module, we find that Petitioner has shown by a preponderance of the evidence that Gupta teaches limitation 1.c.

Limitation 1.d recites, in pertinent part, that “actual vulnerability information” is used in determining “at least one actual vulnerability based on the identified at least one configuration.” Petitioner asserts Gupta teaches “actual vulnerability information” in that Gupta’s “attack file” identifies “computer attacks and countermeasures relevant to the target platform

(block 162)” and “clearly describe[s], in one data structure, what attacks a given environment is vulnerable to.” Pet. 52 (citing Ex. 1004 ¶¶ 164–165). We find “Gupta discloses that the attack file’s actual vulnerability information for the ‘target platform’ or computing ‘environment’ identifies a configuration associated with a plurality of devices as recited in this claim limitation.” See *id.* (citing Ex. 1011 ¶ 179; see also Ex. 1004 ¶ 160 (describing “attack target platforms”). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Gupta teaches limitation 1.d.

Limitation 1.e recites “code for identifying an occurrence in connection with at least one of the plurality of devices.” Petitioner alleges sensor 22 of Gupta’s sensor management system detects an attack on the network. Pet. 53–54 (citing Ex. 1004 ¶ 31 (“The sensor management system 26 may be used to implement a shared-resource virtual intrusion detection system”)). The detection of attacks taught by Gupta falls within the scope of an “occurrence” as “an event that seeks to take advantage of a vulnerability.” See Section III.B.2 above; Pet. 53–54 (citing Ex. 1004 ¶ 83 (“signature processing system *detects attacks*” (emphasis added))). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Gupta teaches limitation 1.e.

Limitation 1.f recites, in pertinent part, the “actual vulnerability . . . is susceptible to being taken advantage of by the occurrence.” We find that Gupta teaches a “hierarchical attack characterization module 150 is used to develop, deploy and manage information on different computer attacks and countermeasures.” See Pet. 55 (citing Ex. 1004 ¶ 154). The characterization module constructs a hierarchy of different computer attacks and

countermeasures. Ex. 1004 ¶ 164. A sensor is downloaded from the characterization module “with the protective software (e.g., the attack file) for the target platform (block 166).” See Pet. 55 (citing Ex. 1004 ¶¶ 164–165). Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that Gupta teaches limitation 1.f.

Limitation 1.g recites, in pertinent part, “providing a user with one or more options to selectively utilize different occurrence mitigation actions . . . including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type . . . utilizing the different occurrence mitigation actions . . . across the plurality of devices.” We find Gupta provides different “occurrence mitigation actions” in its teaching that

[t]he response processor 54 responds to AIDs.^[26] The response processor 54 generates alerts that provide notification of an attack. The response processor 54 also attempts to prevent the attack. *Short-term responses include terminating TCP connections.* Long-term responses include packet logging for further analysis to improve detection and response.

Pet. 57 (citing Ex. 1004 ¶ 87). Petitioner relies on the Nielson Declaration for its testimony that the preceding describes an “intrusion prevention system-based occurrence mitigation technique.” *Id.* at 56 (citing Ex. 1011 ¶ 193 (“terminating TCP connections” is a mitigation action)).

We find the “firewall” type of “occurrence mitigation technique” is taught by Girouard, which discloses first identifying “corrective action.” Pet. 57–58 (citing Ex. 1005 ¶¶ 60–61). Responses taught by Girouard

²⁶ “[T]he classification and pattern matching module 68 raise an AttackID (AID) that indicates the attack that was found in the communications being monitored.” Ex. 1004 ¶ 86.

include installing a software patch and “[a]lternatively, *a firewall policy or security rule may be loaded to a firewall that prevents traffic conforming to a threatening profile from reaching the server.*” *Id.*

Patent Owner disputes that Petitioner has shown limitation 1.g/1.8. PO Resp. 51–59. Patent Owner argues Gupta does not teach providing the “user option” recital, which was discussed in detail in Section III.A.3 above. PO Resp. 52 (citing Ex. 2005 ¶ 78 (graphical user interface (GUI) taught does not have any “option for selecting any mitigation technique”). We find that the GUI allows “user options” through “access [to] *the sensor management system 34 to manage and monitor the VIDS.*”²⁷ See Pet. 56 (citing Ex. 1004 ¶ 143) (emphasis added).

In addition, the Nielson Declaration testimony is that Gupta provides the claimed “user options.” See *id.* (citing Ex. 1011 ¶ 191). Dr. Nielson’s testimony is based, in part, on Gupta’s teaching that “response processor 54 is *configured by the system administrator,*” which after configuration “responds to specific attacks.” Ex. 1011 ¶ 192 (emphasis added) (citing Ex. 1004 ¶ 48).

Dr. Feamster testifies that Gupta’s GUI “never connects to any option for selecting any mitigation technique, much less any user option as specified in this limitation.” Ex. 2005 ¶ 78. We credit Nielson’s opinion testimony over that of Dr. Feamster. The Feamster Declaration is not supported by any teaching of Gupta. To the extent Dr. Feamster cites to Gupta, he references only the mitigation options, not the user option. See *id.*

²⁷ A “virtual intrusion detection system (VIDS) . . . performs local virtual VIDS operations as coordinated by the corresponding VIDS provision module.” Ex. 1004 ¶ 131.

¶ 77. Further, Dr. Feamster does not rebut or otherwise respond to the Nielson Declaration.

Patent Owner next argues that Girouard teaches firewall mitigation but not intrusion prevention mitigation. PO Resp. 53 (citing Ex. 2005 ¶ 80). In addition, Patent Owner contends “Girouard does not disclose that the selection may be made to one or more of the plurality of the devices in the network.” *Id.* at 54 (citing Ex. 1005 ¶¶ 60–61; Ex. 2005 ¶ 81). These arguments are not persuasive because the challenge here relies on Gupta plus Girouard. *See In re Keller*, 642 F.2d 413, 426 (CCPA 1981) (“[O]ne cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references.”). What Patent Owner says is missing from Girouard is taught by Gupta.

Based on the cited argument and evidence, including the Nielson Declaration, we find that Petitioner has shown by a preponderance of the evidence that the combination of Gupta and Girouard teaches limitation 1.g.

(2) Claim 7

Claim 7 depends from claim 1 and recites, in pertinent part, “wherein the computer program product is operable such that different user input is capable of being received prior to the occurrence for different devices, for allowing completion of the different occurrence mitigation actions.” The preceding is the only part of claim 7 Patent Owner identifies as being in dispute. PO Resp. 54 (referencing the quoted part of claim 7 above as limitation 7.1).

Petitioner argues, as it did for claim 1, that both Gupta and Girouard provide the recited “user input” in the form of different occurrence mitigation options. Pet. 59–60 (citing Ex. 1004 ¶¶ 136, 143, 87; Ex. 1004

[1005] ¶¶ 60–61). The Nielson Declaration testimony is cited to show that the subject matter of limitation 7.1 would “enable^[28] one of ordinary skill in the art” to “practice the limitation.” Pet. 61 (citing Ex. 1011 ¶ 207 as support for “disclos[ing] this limitation”).

We have reviewed paragraphs 200 through 206 of the Nielson Declaration, which discuss the teachings of Gupta and Girouard. These paragraphs provide the basis for the opinion expressed in paragraph 207 of the Nielson Declaration. The Nielson Declaration includes testimony that a person of ordinary skill “would also have readily understood that the firewall-based and IPS-based mitigation actions are complementary and can be combined together.” Ex. 1011 ¶ 206. We credit this testimony that “different user input is capable of being received prior to the occurrence for different devices” would have been obvious. Neither Patent Owner nor the Feamster Declaration respond to this testimony or provide any additional evidence for our consideration.

Patent Owner argues²⁹ that the cited paragraphs of Gupta do not teach “a user is provided options to configure and manage the security system, including that a user is provided options to configure and manage the security system.” PO Resp. 55–56 (citing Ex. 2005 ¶ 90). In sum, Patent Owner contends “[n]othing is selectable.” *Id.* at 57. We find that Gupta teaches the “user option” limitation in our discussion of claim 1, limitation

²⁸ As we did above, we understand the Nielson Declaration testimony to be directed to the factual issues underlying obviousness. *See* n.24 above.

²⁹ Patent Owner’s argument at pages 55 through 59 copies verbatim from the Feamster Declaration. *See, e.g.*, PO Resp. 57 (“but what **I** would refer to as preventative or remediation techniques.” (emphasis added)).

1.g above. Patent Owner’s arguments do not add anything further that would cause a change in result.

Patent Owner argues Girouard addresses human process workflow and not mitigation of occurrences. PO Resp. 58 (citing Ex. 2005 ¶¶ 91–92). Thus, Patent Owner argues a person of ordinary skill would not combine Girouard with Gupta. *Id.* We have already found Petitioner has shown a person of ordinary skill would have had sufficient reasons and motivation to combine Gupta and Girouard. Viewing this evidence in light of Patent Owner’s arguments, we maintain that determination.

Petitioner alleges the balance of claim 7 relates to separate occurrence mitigation actions performed on separate devices. *See* Pet. 59. Repeating known steps to obtain a desired result is not inventive. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1330–31 (Fed. Cir. 2009). A known “combination which only unites old elements with no change in their respective functions” would have been obvious. *Great Atl. & Pac. Tea Co. v. Supermarket Equip. Corp.*, 340 U.S. 147, 152–153 (1950). Patent Owner does not contest Petitioner’s characterization or argue patentability based on claim 7’s recitation of separate occurrence mitigation actions performed on separate devices.

Petitioner also argues, invoking section 112, that there is no support in the specification for claim 7 other than claim 7 itself. Pet. 59 (citing Ex. 1011 ¶ 61 (paragraph 61 references claim 1, not claim 7)). Our jurisdiction does not include making a determination of unpatentability under section 112. *See* 35 U.S.C. § 311(b). To the extent Petitioner argues lack of support for the claim, the argument is not available, at least under these circumstances, in an *inter partes* review. Petitioner does not argue

otherwise. Coupled with the lack of any cited legal or factual support, this argument is neither relevant nor persuasive. Given our determination, we need not reach Patent Owner's arguments that the claim is supported. See PO Resp. 54–55.

Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that the combination of Gupta and Girouard teaches claim 7.

(3) Claim 14

Claim 14 depends from claim 1 and recites the following:

code for displaying the one or more options, utilizing at least one user interface; code for receiving a first user input selecting a first one of the options, utilizing the at least one user interface; code for, based on the first user input, automatically applying a first one of the different occurrence mitigation actions of the firewall-based occurrence mitigation type; code for receiving a second user input selecting a second one of the options, utilizing the at least one user interface; and code for, based on the second user input, automatically applying a second one of the different occurrence mitigation actions of the intrusion prevention system-based occurrence mitigation type.

Petitioner asserts that claim 14 adds limitations to claim 1 “requiring code for receiving a first user input selecting a firewall-based occurrence mitigation type and a second user input selecting an intrusion prevention system-based occurrence mitigation type.” Pet. 61. Petitioner relies on the same evidence and argument it did in challenging claim 7. *Id.* at 61–62 (citing Ex. 1004 ¶¶ 136, 143; Ex. 1004 [1005] ¶¶ 60–61; Ex. 1011 ¶¶ 211, 215, 217).

Patent Owner does not dispute Petitioner's summary of claim 14 and argues claim 14 is not unpatentable for the same reasons as claim 7. PO Resp. 59–60. The Feamster Declaration is a copy of the Patent Owner

Response and adds nothing beyond claim 7 arguments. *See* Ex. 2005 ¶¶ 98–100.

As was the case with claim 7, the subject matter of claim 14 is substantially the same as claim 1 and our analysis there applies equally here. Based on the cited argument and evidence, we find that Petitioner has shown by a preponderance of the evidence that the combination of Gupta and Girouard teaches claim 14.

d. Summary of Obviousness over Gupta and Girouard

Petitioner’s argument and supporting evidence have shown by a preponderance of the evidence that the subject matter of claims 1, 7, and 14 would have been obvious over Gupta and Girouard.

5. Obviousness of Claims 1, 7, and 14 Over Gleichauf and Hill (Ground 4)

Petitioner argues claims 1, 7, and 14 would have been obvious under § 103 over Gleichauf and Hill. Pet. 62–75. Petitioner’s argument is supported by the Nielsen Declaration. Ex. 1011 ¶¶ 226–301. Patent Owner relies on our Institution Decision, which preliminarily found Gleichauf and Hill did not render any of claims 1, 7, or 14 obvious. PO Resp. 61 (citing Inst. Dec. 40–42). In the Institution Decision we preliminarily determined that Petitioner had not sufficiently shown that Gleichauf teaches limitation 1.b. Inst. Dec. 40–42.

a. Overview of Gleichauf (Ex. 1006)

Gleichauf discloses

A method and system for adaptive network security using network vulnerability assessment is disclosed. The method comprises directing a request onto a network. A response to the request is assessed to discover network information. A plurality of analysis tasks are prioritized based upon the network

information. The plurality of analysis tasks are to be performed on monitored network data traffic in order to identify attacks upon the network.

Ex. 1006, Abstract.

The network security system “can make an assessment of potential vulnerabilities 80 associated with each device on internal network 10.”

Ex. 1006, 7:57–60. A “priority engine . . . use[s] the information in network map 28 to prioritize the analysis tasks to be performed on monitored traffic by protocol engine 24 and signature engine 26.” *Id.* at 7:62–65.

b. Overview of Hill (Ex. 1003)

An overview of Hill appears in Section III.D.3.b above.

c. Analysis—Obviousness of Claims 1, 7, and 14 over Gleichauf and Hill

Limitation 1.b recites in pertinent part, “actual vulnerability information.” Petitioner argues “a person of ordinary skill would understand the network map as disclosed by Gleichauf to be ‘actual vulnerability information.’” Pet. 64 (citing Ex. 1011 ¶ 239). As to that part of limitation 1.b reciting “first data storage” and “second data storage,” Petitioner argues a person of ordinary skill would have understood “that Gleichauf’s network map (i.e., a first data storage) is generated based on potential vulnerabilities associated with devices (i.e., a second data storage).” *Id.* (citing Ex. 1011 ¶ 243).

Patent Owner’s Preliminary Response argued “Petitioner either does not point to an element that teaches a first data storage, or does not point to an element that teaches actual vulnerability information.” Prelim. Resp. 39. In our Institution Decision we found Patent Owner argued persuasively that Gleichauf’s “network map” cannot be both “actual vulnerability

information” and a “first data storage.” Inst. Dec. 41 (citing Prelim. Resp. 39). We declined to institute trial on this ground, reinstating it after SAS. Inst. Dec. 42; Mod. Inst. Dec. 2.

The Institution Decision preliminarily determined that Gleichauf’s “network map” cannot be interpreted to be both “actual vulnerability information” and “first data storage.” We stated the Petition clearly relies on the “network map” teaching of Gleichauf to teach both limitations. Pet. 64. While the “network map” may have multiple functions, Petitioner does not sufficiently explain how those separate functions meet both limitations. See Ex. 1006, 7:57–65. Our rules require that “the petition must specify where each element of the claim is found in the prior art patents.” See 37 C.F.R. § 42.104(b)(4).

Patent Owner’s Response simply restated, without any further arguments, what we determined in the Institution Decision. PO Resp. 61. The Petitioner’s Reply explained that the Petition

did not assert that the disclosure of Gleichauf’s network map is both “actual vulnerability information” and “first data storage.” Rather, on page 64 the Petition asserted Gleichauf discloses a network map containing “actual vulnerability information” that is stored in a “first data storage,” and that the network map is generated based upon “potential vulnerability information” that is stored in a “second data storage”

Pet. Reply 29; *see also* Pet. 64 (citing Ex. 1001 ¶ 239). As to a second data storage of potential vulnerability information, Petitioner points to the Nielson Declaration testimony that a person of ordinary skill “would understand that Gleichauf’s network map (i.e., a first data storage) is generated based on potential vulnerabilities associated with devices (i.e., a second data storage).” Pet. Reply 29 (citing Ex. 1011

¶ 243); Pet. 64. This argument was repeated at oral hearing. Tr. 32:1–9.

We are not persuaded by Petitioner’s argument. Petitioner does not address our determination in the Institution Decision that the network map of Gleichauf cannot be both “actual vulnerability information” and “first data storage.” Petitioner simply restates its showing that we found lacking in the Institution Decision.

Petitioner has not shown by a preponderance of the evidence that Gleichauf teaches limitation 1.b.

d. Summary of Obviousness over Gleichauf and Hill

Petitioner’s argument and supporting evidence have not shown by a preponderance of the evidence that claim 1, and, therefore, claims 7 and 14, would have been obvious over Gleichauf and Hill.

IV. ORDER

In consideration of the foregoing, it is
ORDERED that claims 1, 7, and 14 of the ’644 patent are held
unpatentable;

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

FOR PETITIONER:

Robert Hansen
Timothy Murphy
Shaun Gregory
THE MARBURY LAW GROUP, PLLC
bhansen@marburylaw.com
tjmurphy@marburylaw.com
sgregory@marburylaw.com

FOR PATENT OWNER:

Thomas Kramer
O'KELLY ERNST & JOYCE, LLC
tkramer@oelegal.com

Thomas Meagher
Alan Pattillo
MEAGHER EMANUEL LAKS GOLDBERG & LIAO, LLP
tmeagher@meagheremanuel.com
cpattillo@meagheremanuel.com