UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

FORESCOUT TECHNOLOGIES, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

_____

Case IPR2021-01328
Patent US 9,503,421 B2

_____

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

Pursuant to 35 U.S.C. § 313 and 37 C.F.R. § 42.107, Fortinet, Inc. ("Patent Owner") hereby provides a preliminary response to Forescout Technologies, Inc.'s ("Petitioner") Petition to institute *inter partes* review of Claims 1, 4-10, 15, and 18-24 of U.S. Patent No. 9,503,421 B2 (the "'421 Patent"). Paper 1 (the "Petition" or "Pet."). The Petition fails to demonstrate a reasonable likelihood that any challenged claim of the '421 Patent is unpatentable. The Board should deny institution.

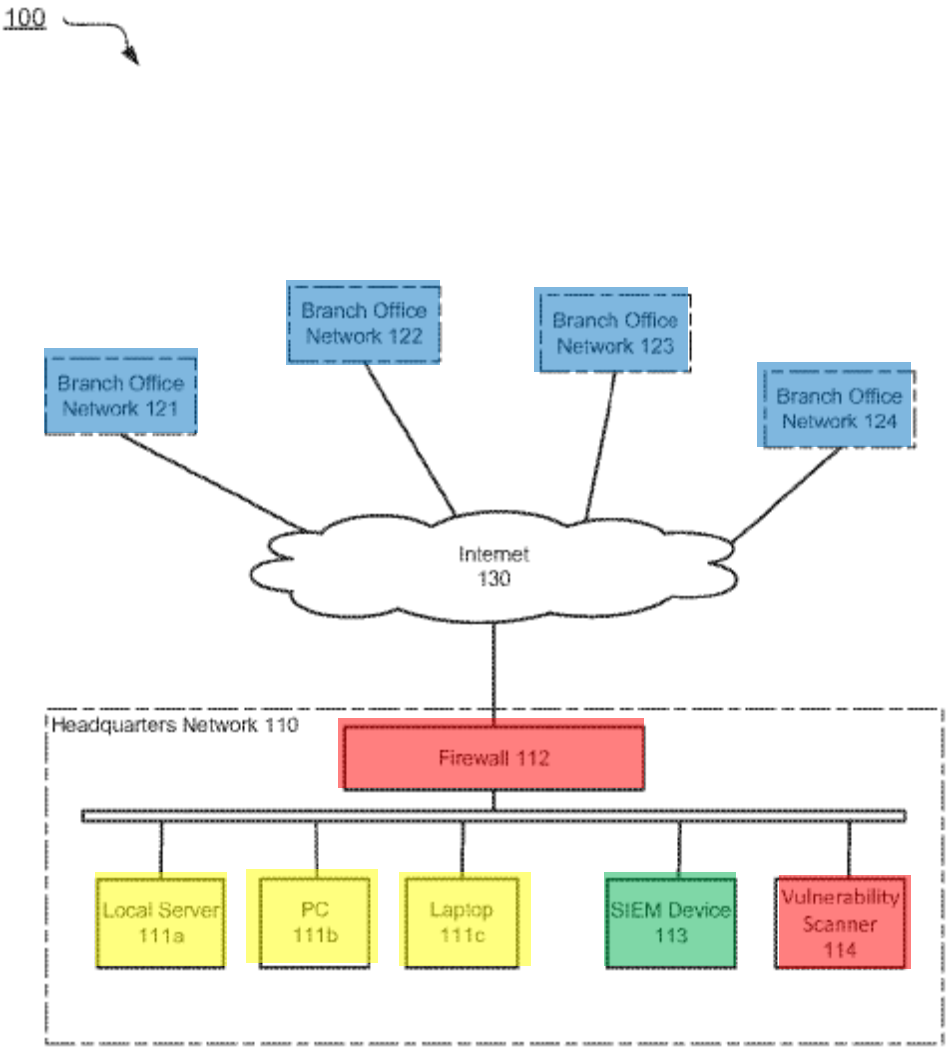
As a threshold matter, the Board should deny institution because the Petition fails to demonstrate that U.S. Patent No. 10,129,290 B2 to Thomas et al. ("Thomas") (EX-1004) is prior art. Because both Grounds 1 and 2 rely on Thomas, the Board should deny institution for this reason alone. The Board should also deny institution on both grounds because the Petition fails to demonstrate that Thomas discloses "creating" a work flow, as required by independent Claims 1 and 15.

II. The '421 PATENT

A. Background of the '421 Patent

The '421 Patent is directed to "[s]ystems and methods . . . for conducting work flows by an SIEM device to carry out a complex task automatically." EX-1001, Abstract. Figure 1 illustrates a network architecture 100 that includes security information and event management (SIEM) device 113 (annotated in green), firewall

112 and vulnerability scanner 114 (both annotated in red), and multiple branch office networks 121, 122, 123, 124 (all annotated in blue):



EX-1001, FIG. 1 (annotated), 5:1-19. In this network, the SIEM device (annotated in green) "schedule[s] vulnerability scanner 114 [(annotated in red) as well as] other vulnerability scanners of branch office networks 121-124 to scan computing/networking devices of the networks for vulnerabilities." EX-1001, 5:20-24. Local server 111a, PC 111b, and laptop 111c (all annotated in yellow) are

examples of "network appliances [that are] operatively coupled to each other through a Local Area Network (LAN), wherein the LAN is then operatively coupled with [the] firewall 112 that enables access to Internet 130." EX-1001, 5:5-10.

Figure 2 below illustrates functional units of a SIEM device, such as SIEM device 113, which includes a manager layer 210 (annotated in red), an engine layer 230 (annotated in blue), a device adapter layer 250 (annotated in green) and a device layer 270 (annotated in yellow)":

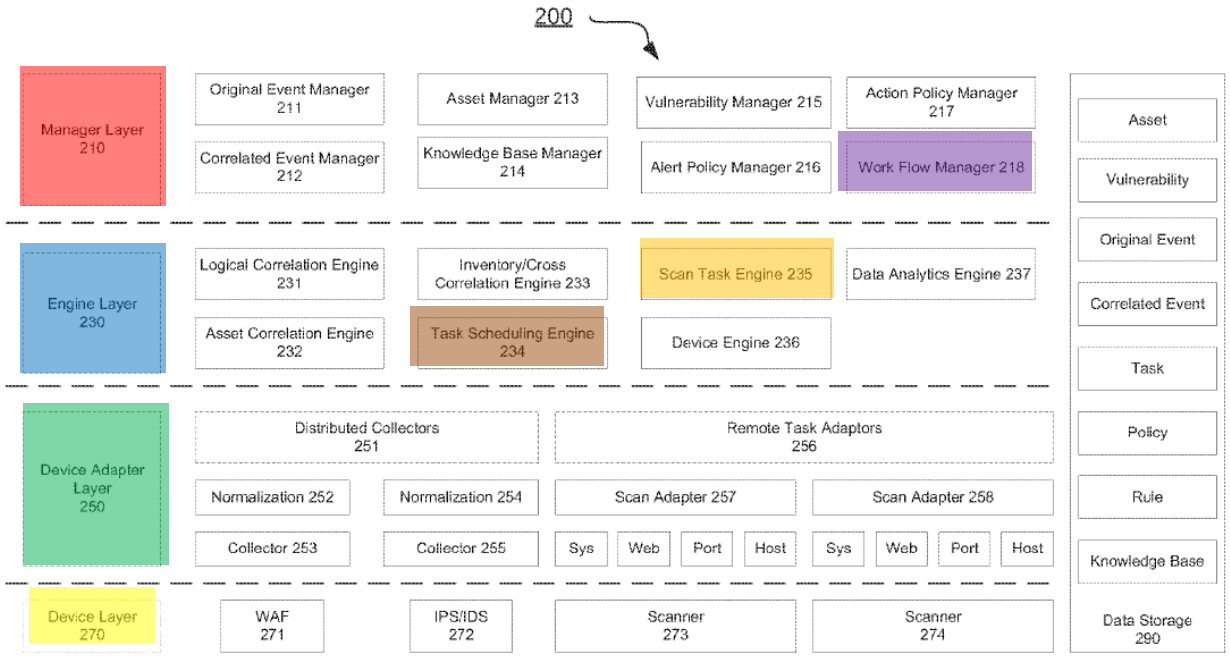


FIG. 2

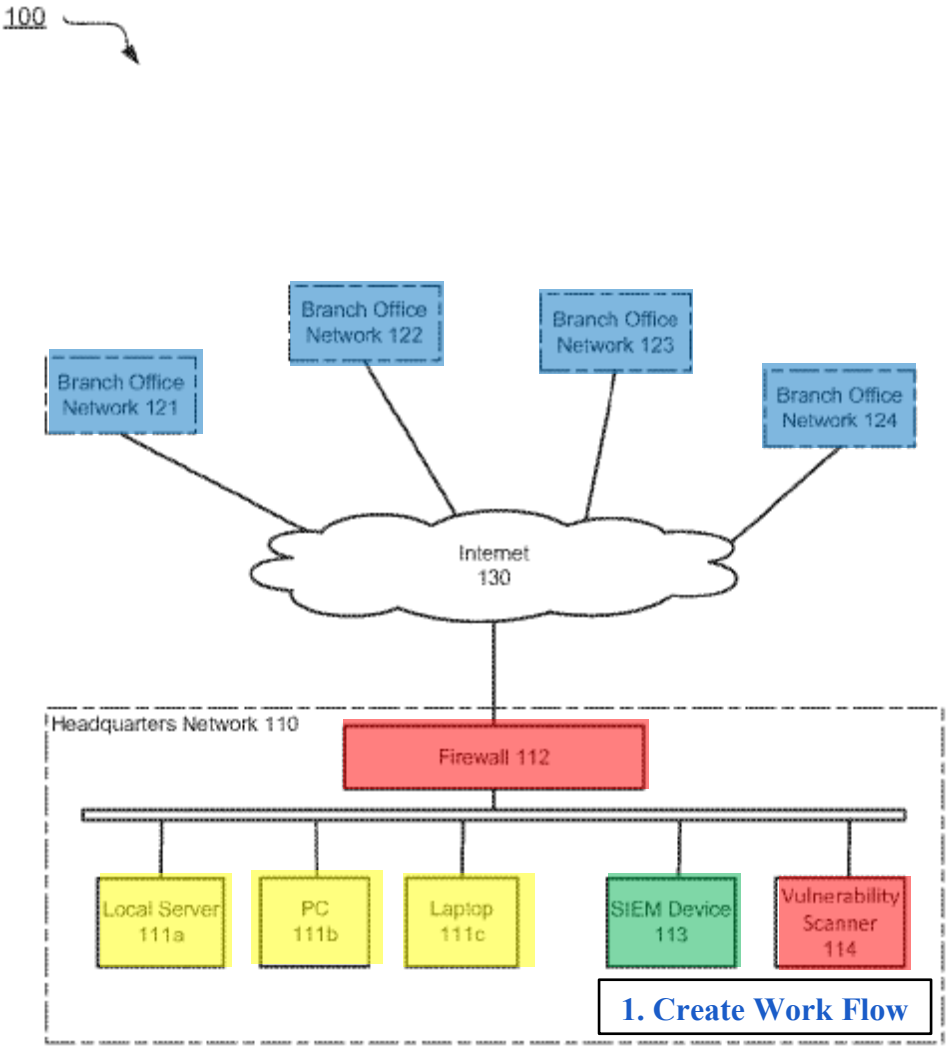
EX-1001, FIG. 2 (annotated), 6:23–27. Among other functional units, the management layer 210 (annotated in red) includes a work flow manager 218 (annotated in purple) that "create[s] a work flow by specifying a series of commands/instructions that are carried out by multiple security devices," where

"[e]ach one in the series of commands/instructions designates a specific task, a host that conducts the specific task and optional parameters needed to conduct the task." EX-1001, FIG. 2, 8:25-31; *see also* EX-1001, 1:52-54 (disclosing the "SIEM device may create a work flow that includes multiple tasks"), 2:36-40 (disclosing the "SIEM device may create a work flow or work flow template"), 2:45-47 (same). The parameters may include, for example, "logic conditions for triggering the task." EX-1001, FIG. 2, 8:32-33.

The engine layer 230 (annotated in blue) includes, among other functional units, a task scheduling engine 234 (annotated in brown) and a scan task engine 235 (annotated in orange). The task scheduling engine 234 (annotated in brown) "launch[es] work flows at the times designated by the work flow policies," and "sen[ds them] to task engine 235 for execution." EX-1001, FIG. 2, 10:32-36. The scan task engine 235 (annotated in orange) can "driv[e] the execution of tasks and [also] collect[s] results of tasks after tasks are executed." EX-1001, FIG. 2, 10:45-46.

The capability to create, schedule, and execute a work flow allows the SIEM device to "link multiple security tasks together to accomplish a complex task automatically even though these tasks may be conducted by different security devices potentially from different manufacturers." EX-1001, 8:33-37. For example, the '421 Patent describes a process by which an SIEM device creates and executes

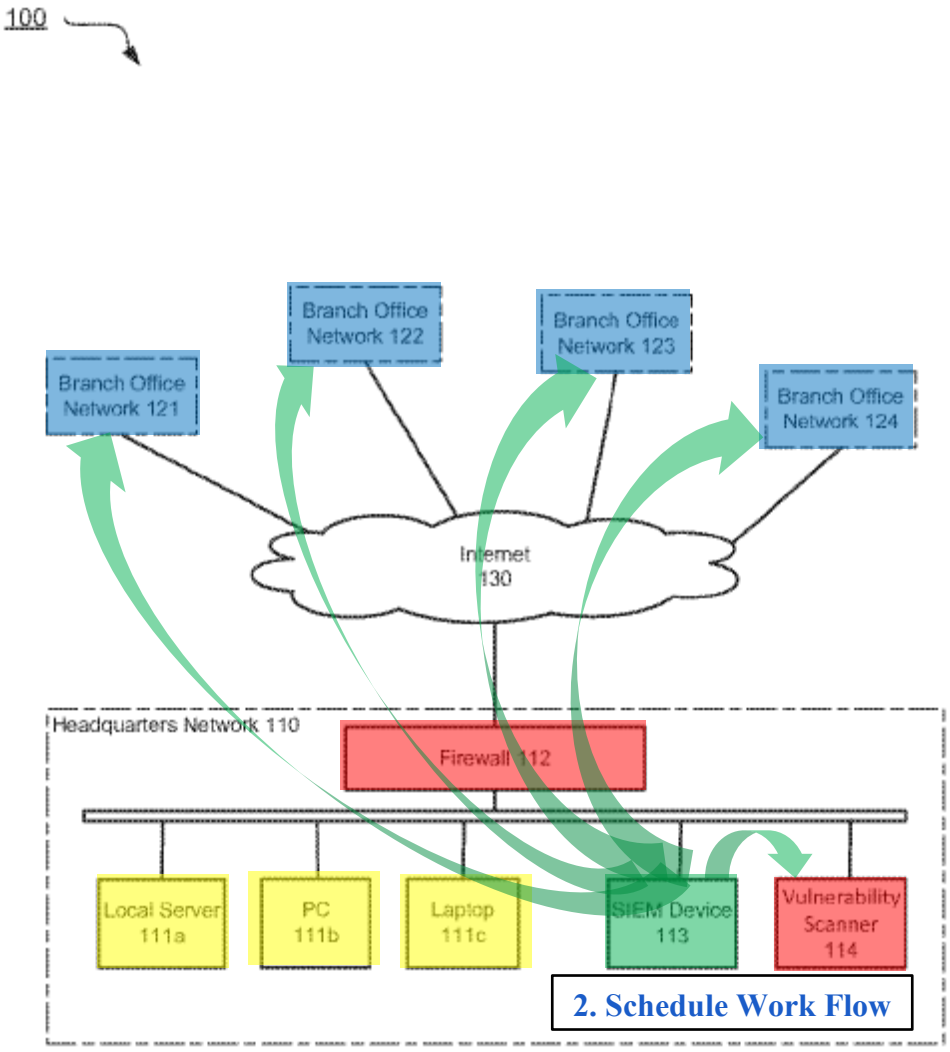
a work flow, including a work flow template, which "defines abstract tasks that may be conducted by multiple security devices." EX-1001, 12:9-39. The '421 Patent discloses that the work flow created by the SIEM can be "a set of commands/instructions that can be carried out by security devices together with parameters or logical conditions for the execution of commands/instructions." EX-1001, 13:23-26. The process begins when a work flow template is created and then "dynamically creating a work flow instance" that includes specific tasks derived from the work flow template. EX-1001, 12:22-44, FIG. 3 (steps 301, 302). The '421 Patent discloses that "[b]y using work flow templates and dynamically creating a work flow instance when scheduled, an SIEM device has more flexibility to use various security devices from different manufacturers." EX-1001, 12:32-35.



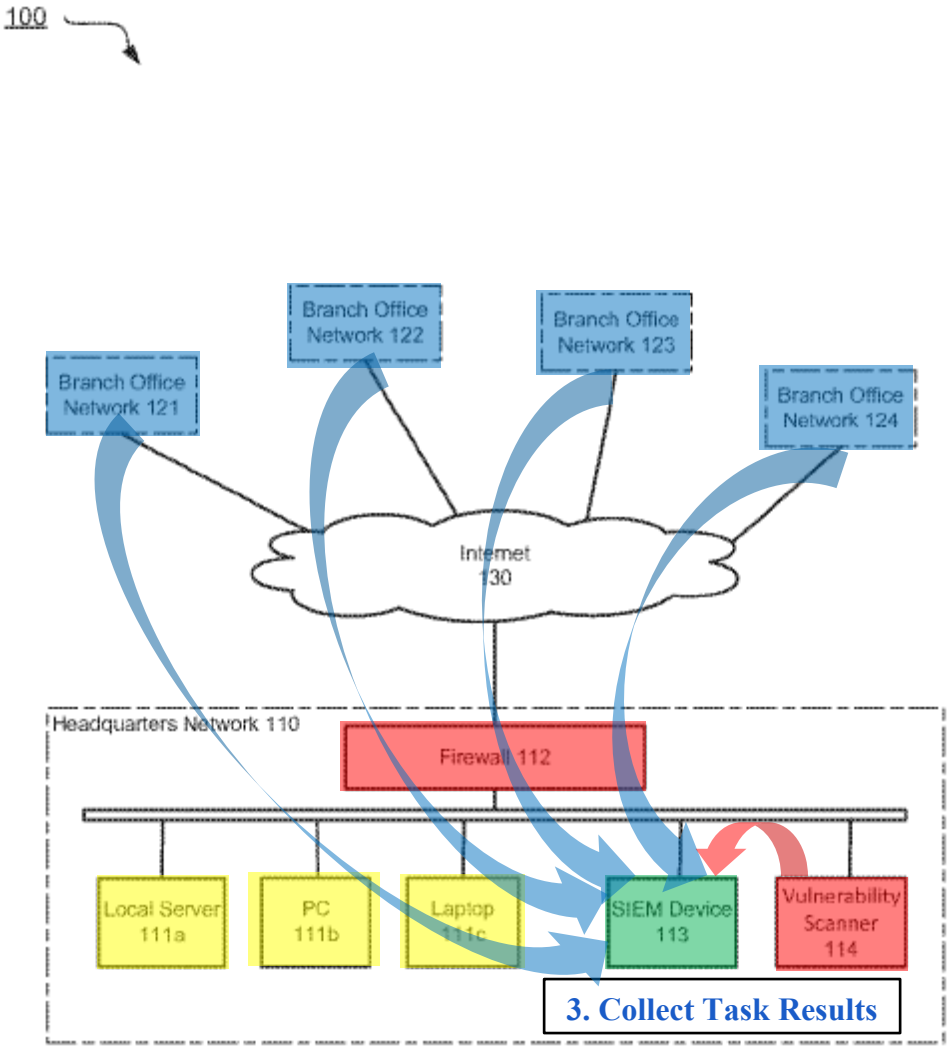
EX-1001, FIG. 1 (annotated).

The ’421 Patent further discloses that the “work flow template is scheduled for execution” and the “work flow instance or specific tasks are derived from the work flow template by translating the abstract tasks in the work flow template into specific tasks that can be executed by specific security devices.” EX-1001, 12:40-61, FIG. 3 (steps 302, 303). The work flow is scheduled by transmitting the task and any required parameters to the multiple security devices (depicted as green

arrows), which then execute the scheduled tasks, for example, sequentially or concurrently:



EX-1001, FIG. 1 (annotated). The SIEM device collects the "execution results of tasks" (depicted as red and blue arrows), and "may also report the execution results of the work flow to an administrator of the SIEM device":



Ex-1001, FIG. 1 (annotated), 12:63-13:17, FIG. 3 (steps 304, 305). As such, the claimed invention provides for creating, scheduling, and executing multiple tasks of various security devices (e.g., vulnerability scanner 114 (red), vulnerability scanners of branch office networks 121-124 (blue)) by which the SIEM device not only creates work flows, but also schedules and executes work flows; and thereby automatically achieving comprehensive security information and event management of a network. EX-1001, FIG. 1, FIG. 3, 1:52-54, 2:36-40, 2:45-47, 12:63-13:17.

B. The Challenged Claims and Asserted Grounds

Petitioner challenges Claims 1, 4-10, 15, and 18-24 (the "Challenged Claims") as obvious over Thomas in view of the knowledge of a person of ordinary skill in the art ("POSA") (Ground 1) and Claims 4-8 and 18-22 as obvious over Thomas in view of U.S. Patent Appl. Pub. No. 2012/0224057 to Gill (EX-1006) (Ground 2). Pet. 7-8.

Of the Challenged Claims, Claims 1 and 15 are the only independent claims, and the remaining Challenged Claims 4-10 and 18-24 depend from Claim 1 or Claim 15. Claim 1 is a method and Claim 15 is a corresponding SIEM system for performing the method of Claim 1 as shown below:

1. A method comprising: ***creating, by a security information and event management (SIEM) device associated with a private network, a work flow****, said work flow including information defining a plurality of security tasks that are to be performed by one or more security devices associated with the private network and managed by the SIEM device, wherein the plurality of security tasks include operations that are intended to*	*15. A security information and event management (SIEM) system comprising:* *non-transitory storage device having embodied therein instructions representing a security application; and* *one or more processors coupled to the non-transitory storage device and operable to execute the security application to perform a method comprising:*

protect the private network against attacks; *starting, by the SIEM device, the work flow by scheduling the one or more security devices to perform the plurality of security tasks defined in the work flow; and* *collecting, by the SIEM device, results of the plurality of security tasks after they are performed by the one or more security devices.*	***creating a work flow**, said work flow including information defining a plurality of security tasks that are to be performed by one or more security devices associated with a private network and managed by the SIEM system, wherein the plurality of security tasks include operations that are intended to protect the private network against attacks;* *starting the work flow by scheduling the one or more security devices to perform the plurality of security tasks defined in the work flow; and* *collecting results of the plurality of security tasks after they are performed by the one or more security devices.*

EX-1001, 18:18-33 (Claim 1), 19:21-40 (Claim 15).

The limitations bolded in **red** above are referred to as the "creating a work flow" limitation in this Preliminary Response.

III. PRIORITY DATE OF THE CHALLENGED CLAIMS

The priority date of the Challenged Claims is not disputed.

IV. KNOWLEDGE OF A PERSON OF ORDINARY SKILL IN THE ART

To narrow the issues for purposes of this Preliminary Response, Patent Owner does not dispute Petitioner's definition of a POSA relevant to the '421 Patent.[1]

V. CLAIM CONSTRUCTION

For purposes of this Preliminary Response, Patent Owner asserts that the claim terms be given their plain and ordinary meaning.

VI. THE BOARD SHOULD DENY INSTITUTION OF ALL GROUNDS.

Petitioner has failed to meet its burden of establishing a reasonable likelihood that any Challenged Claim is unpatentable under any ground for at least the following reasons: (1) Thomas, the primary reference Petitioner relies upon in both grounds, is not prior art; and (2) Thomas does not disclose the "creating a work flow" limitation.

A. The Disclosure of Thomas

Thomas is titled "Dynamic Adaptive Defense for Cyber-Security Threats" and relates to a "cyber-security system [that can] provide enhanced capability to operate effectively, mitigate threats, survive breaches, and maintain operations during attacks." EX-1004, (54), Abstract. The system, "[u]pon recognition of a

[1] Patent Owner reserves the right to dispute Petitioner's definition of a POSA as a technological matter and consistent with Patent Owner's positions in other related proceedings.

cyber-security threat, through preconfigured activation workflow plans, [can] automatically provide[] system configuration instructions to defend against threats originating both external to and internal to the network." EX-1004, Abstract.

Petitioner contends that Thomas provides a cyber-data management node 104 (annotated in yellow) that is "configured to ingest internet protocol (IP) and other data for analysis to determine acceptance/denial in [a] network as well as dealing with disparate data and transforming it into an understandable and meaningful database for logical analysis":

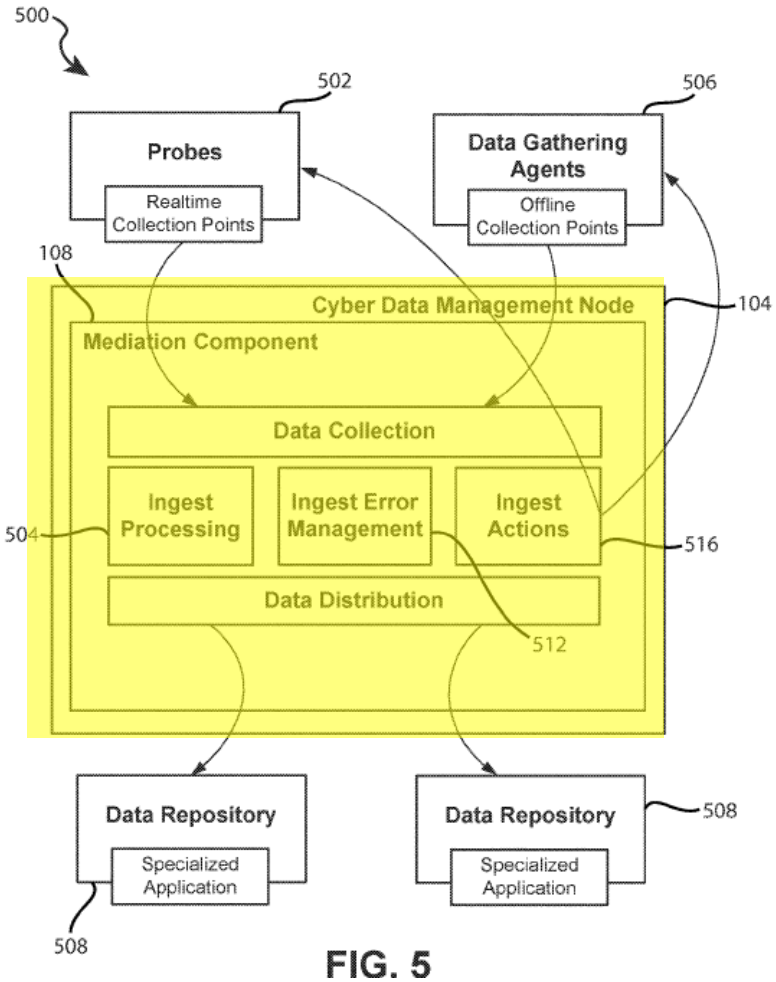


FIG. 5

EX-1004, FIG. 5 (annotated); Pet. 11 (citing EX-1004, 8:13-21). According to Petitioner, the cyber-data management node 104 can "initiate one or more automated workflows" when responding to cyber-security threats, where a workflow "includes actions . . . or action plans which are specifically targeted towards security incident remediation." Pet. 12-13 (citing EX-1004, 8:13-21).

The cyber-data management node includes a mediation component 108 (annotated in red) "that is configured to ingest, enrich, and analyze data regarding cyber-security alerts and threats" and an activation component 116 (annotated in blue) that "is configured to respond to manual triggers and/or triggers received from the mediation component 108 [(annotated in red)] by controlling and/or managing disparate network elements":

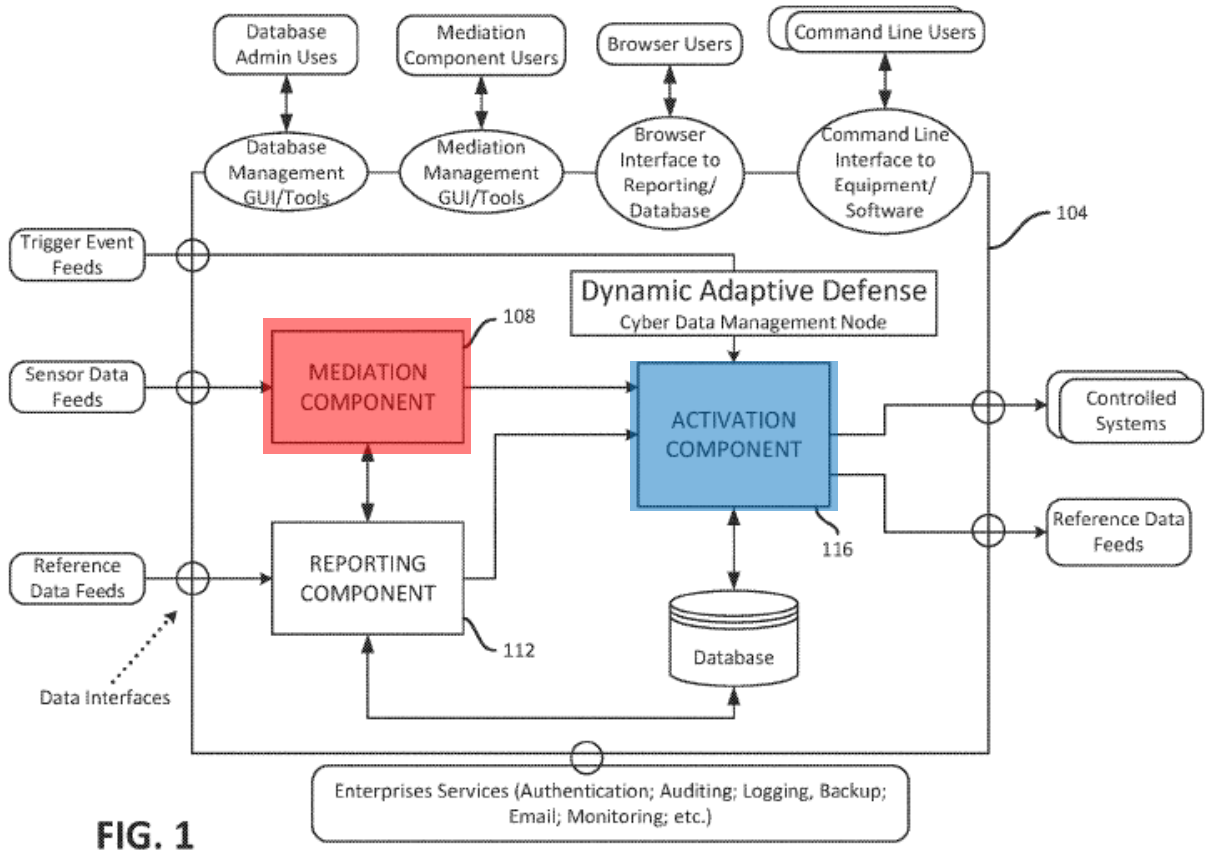


FIG. 1

EX-1004, FIG. 1 (annotated); Pet. 11 (citing EX-1004, 8:13-21); EX-1004, 8:30-33. The mediation component 108 (annotated in red) may "receive information from a variety of commercial and proprietary sensors and upstream systems in a variety of formats," and can route "sensor information" to the activation component 116 "for workflow purposes." EX-1004, 14:9-18. The activation component 116 can then "initiate pre-configured workflows," where a workflow "may initiate an action directly, or may be queued for selection in a reporting module by an end user." EX-1004, 14:18-23.

B. The Petition Fails to Demonstrate that Thomas is Prior Art.

As a threshold matter, the Board should deny institution because Petitioner fails to demonstrate that Thomas is prior art. In particular, Petitioner has failed to establish that Thomas is entitled to the benefit of priority to the filing date of its provisional application, which would be required to qualify as prior art to the Challenged Claims.

Petitioner contends that Thomas is prior art because it is entitled to claim priority to U.S. Provisional Application 61/944,019 (the "Thomas Provisional"), which was filed on Feb. 24, 2014.[2] Pet. 14 (arguing "Thomas is prior art because it contains a priority claim to the Thomas Provisional, was filed within the applicable filing period, and has a common inventor"), 21 (arguing that "[b]ecause the filing date of the Thomas Provisional (Feb. 24, 2014) precedes the earliest effective filing date of the '421 patent (Mar. 17, 2014), Thomas is prior art"); EX-1004, (60);

[2] The non-provisional application for the '421 patent (U.S. Patent Application No. 14/215,333) was filed on March 17, 2014, which, for purposes of this Preliminary Response, Patent Owner does not dispute is the priority date for the Challenged Claims. EX-1001, (17); Pet. 4. The non-provisional application for Thomas was filed on April 1, 2016, which is after the March 17, 2014 priority date. EX-1004, (17).

EX-1005, 1. Petitioner argues that "[a]lthough no need exists to evaluate whether Thomas is entitled to claim priority to the Thomas Provisional, such an analysis shows that at least one claim of Thomas is supported by the Thomas Provisional" and "Dr. Cole's analysis shows that the Thomas Provisional provides written description and enablement support for at least claim 11 of Thomas." Pet. 15.

To establish that a reference patent is entitled to the benefit of its provisional application's filing date for prior art purposes, a petitioner has the burden to show that the following two requirements are met. First, a petitioner must show that the provisional application provides sufficient support for at least one claim in the reference patent. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1385, 1382 (Fed. Cir. 2015) ("A provisional application's effectiveness as prior art depends on its written description support for the claims of the issued patent of which it was a provisional."); *Ex parte Mann*, 2016 WL 7487271, at *6 (P.T.A.B. Dec. 21, 2016) (explaining whether *Dynamic Drinkware* requires "support in the provisional . . . for *all* claims, *any* claim, or something in between").

Second, a petitioner must show that the provisional application provides sufficient support for the subject matter relied upon for prior art purposes in the reference patent. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010) (requiring that the relied upon subject matter "was carried forward from an earlier U.S. provisional application or U.S. non-provisional application"); *Cox*

Communications, Inc. v. AT&T Intellectual Property I, L.P., IPR2015-01227, Paper 70 at 29 (P.T.A.B. Nov. 16, 2015) ("[T]he material relied upon as teaching the subject matter of the challenged claims must be carried through from that earlier filed application to the reference patent being used against the claim.") (citing *Giacomini*, 612 F.3d at 1383); *Ex parte Mann*, 2016 WL 7487271, at *5 (P.T.A.B. Dec. 21, 2016) (explaining that "[t]his subject matter test is in addition to the comparison of claims required by *Dynamic Drinkware*," and that "absurd results would be reached if a subject matter test were not required"); *Comcast Cable Commc'ns, LLC v. Promptu Sys. Corp.*, IPR2018-00345, Paper 10 at 25-26 (P.T.A.B. July 2, 2018) (finding Petitioner's analysis insufficient to show "how the [provisional application] provides support for the subject matter relied upon [in the asserted reference]"). The MPEP also provides that "a U.S. patent document is effective as prior art as of the filing date of the earliest application to which benefit or priority is claimed and which describes the subject matter relied upon." MPEP § 2151 (9th Ed., Rev. 10.2019, June 2020).

Petitioner fails to meet its burden. Petitioner has failed to show that the disclosures of Thomas upon which Petitioner relies as teaching the subject matter of the Challenged Claims were disclosed in and "carried forward" from the earlier Thomas Provisional, and thus that Thomas is prior art. *Giacomini*, 612 F.3d at 1383. The Board should therefore deny institution.

Although Petitioner purports to address the first requirement, alleged support in the Thomas Provisional for at least one claim of Thomas (Pet. 14-21), Petitioner fails to address (or even acknowledge) the second requirement: whether the Thomas Provisional provides sufficient support for the subject matter relied upon for prior art purposes in Thomas. Petitioner ignores this requirement.

Petitioner makes no meaningful attempt to establish that the relied upon portions of Thomas are in fact supported by the Thomas Provisional. Instead, Petitioner seeks the benefit of the Thomas Provisional's filing date by merely attempting to show that the Thomas Provisional provides support for at least one claim in Thomas, and then Petitioner relies upon some other disclosures in Thomas that do not appear or have support in the Thomas Provisional.

For example, Petitioner relies upon Thomas's Figure 10 as allegedly disclosing subject matter of the Challenged Claims. *See* Pet. 25–26, 30, 47. In particular, regarding the "associated with a private network" limitation of Claims 1 and 15, Petitioner identifies and relies on Figure 10 of Thomas and accompanying disclosures about Figure 10 in Thomas's specification. Pet. 25-26 (identifying EX-1004, FIG. 10, 19:26-28), 47 (relying on "the same reasons as [C]laim 1" for Claim 15).

Figure 10 of Thomas, however, is not found in the Thomas Provisional. In fact, the Thomas Provisional includes only nine figures, labeled as figures 1 through

9, and does not disclose or describe a figure 10. *See generally* EX-1005. Petitioner does not allege or make any attempt to show that any of the figures or other disclosures in the Thomas Provisional describe or correspond to the relied-upon disclosure in Figure 10 of Thomas. Although Petitioner states that "Thomas teaches that '[t]he perimeter 712 separates the enterprise 708 from external networks such as the Internet 704'" (Pet. 25 (quoting EX-1004, 19:26-28)), that same disclosure does not appear in the Thomas Provisional. Petitioner also does not explain how or why the Thomas Provisional provides support for the disclosure in Figure 10 of Thomas relied upon in the Petition.

Similarly, Petitioner relies on Figure 15A of Thomas as allegedly disclosing subject matter of the Challenged Claims. Pet. 28-30, 33, 35, 38, 47. For example, regarding the "said work flow including information defining a plurality of security tasks that are to be performed by one or more security devices associated with the[/a] private network" limitation of Claims 1 and 15, Petitioner identifies and relies on Figure 15A of Thomas and accompanying disclosures about Figure 15A in Thomas's specification. Pet. 28-29 (identifying EX-1004, FIG. 15A, 27:34-42), 47 (relying on "the same reasons as [C]laim 1" for Claim 15). Petitioner contends:

> "FIG. 15A shows a sequencing diagram 1501 that shows several actions 1552 being associated with certain network elements 1556. When action sets for the interactive sequencing diagram 1501 are created, those that are to run

> in parallel or otherwise as a group can be displayed in the sequencing map of FIG. 15A as a grouping. . . . For example, the grouping that runs first can be displayed on the far left, the subsequent group just to the right of first group, and so on."

Pet. 28 (quoting EX-1004, 27:37-42).

But, like Figure 10 of Thomas, Figure 15A and the disclosure at column 27, lines 34-42 of Thomas Petitioner identifies and relies upon are found nowhere in the Thomas Provisional. *See generally* EX-1005. Although in a footnote at page 17 of the Petition, Petitioner seems to allege that Figure 15A of Thomas and Figure 7A of the Thomas Provisional are somehow "the same drawings," Petitioner does not identify evidence or provide any meaningful explanation to support such allegation. In particular, Petitioner does not meaningfully explain how or why Figure 7A or any alleged disclosures about Figure 7A in the Thomas Provisional provide sufficient support for Thomas's Figure 15A relied upon in the Petition. The mere fact that the figures may appear to be similar in some respects, without more, is insufficient. *See New Railhead Mfg., L.L.C. v. Vermeer Mfg. Co.*, 298 F.3d 1290, 1294-95 (Fed. Cir. 2002) (affirming decision where drawings in provisional application were found insufficient to support non-provisional application's claim of priority). Petitioner's conclusory assertion that "the same drawings are present as Figure 15 in Thomas" (Pet. 17 n.4) is equally insufficient.

Additionally, Petitioner relies upon disclosures in columns 20-22 and 27 of Thomas as allegedly disclosing subject matter of the Challenged Claims. *See* Pet. 26 (citing EX-1001, 20:4-6), 27 (citing EX-1001, 22:10-18), 27 (citing EX-1004, 21:4-6), 28 (citing EX-1001, 27:37-42), 35 (citing EX-1004, 27:34-40, 27:40-42). For example, regarding the "wherein the plurality of security tasks of the work flow are performed serially" limitation of Claims 4 and 18, Petitioner relies on Thomas's disclosures at column 27, lines 34-42. Pet. 34-35, 47. Yet, Petitioner makes no attempt to show that these relied-upon disclosures are disclosed in and carried forward from the Thomas Provisional, and likewise makes no such showing for the relied-upon disclosures in columns 20-22 of Thomas. *See generally* Pet. 26-28, 34-35, 47. Petitioner does not identify any corresponding disclosures in the Thomas Provisional or explain how any such disclosures provide requisite support for the relied-upon disclosures in columns 20-22 and 27 of Thomas.

Petitioner's approach essentially requires Patent Owner (and the Board) to guess as to what Petitioner might have argued had it attempted to explain how the Thomas Provisional provides support for the alleged subject matter of Thomas relied upon in the Petition. That approach does not satisfy Petitioner's burden. *See Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.*, 853 F.3d 1272, 1286 (Fed. Cir. 2017) ("It is of the utmost importance that petitioners in the IPR proceedings adhere to the

requirement that the initial petition identify with particularity the evidence that supports the grounds for the challenge to each claim.").

Because Petitioner has failed to establish the second requirement—that the Thomas Provisional provides sufficient support for the relied upon disclosures of Thomas—Thomas is not entitled to the benefit of priority to the filing date of the Thomas Provisional, and thus Petitioner has failed to establish that Thomas is prior art and likewise has failed to demonstrate a reasonable likelihood that the Challenged Claims are unpatentable under Grounds 1 and 2.

C. The Petition Fails to Demonstrate that Thomas Discloses the "Creating a Work Flow" Limitation.

Even if Thomas were entitled to claim priority to the Thomas Provisional, Thomas does not disclose the "creating a work flow" limitation. Petitioner contends that Thomas discloses the "creating a work flow" limitation of Challenged Claims 1 and 15 by Thomas's activation component 116. Pet. 22-30.

By way of background, Petitioner identifies Thomas's cyber-data management node 104 as the claimed "SIEM" device/system (annotated in yellow):

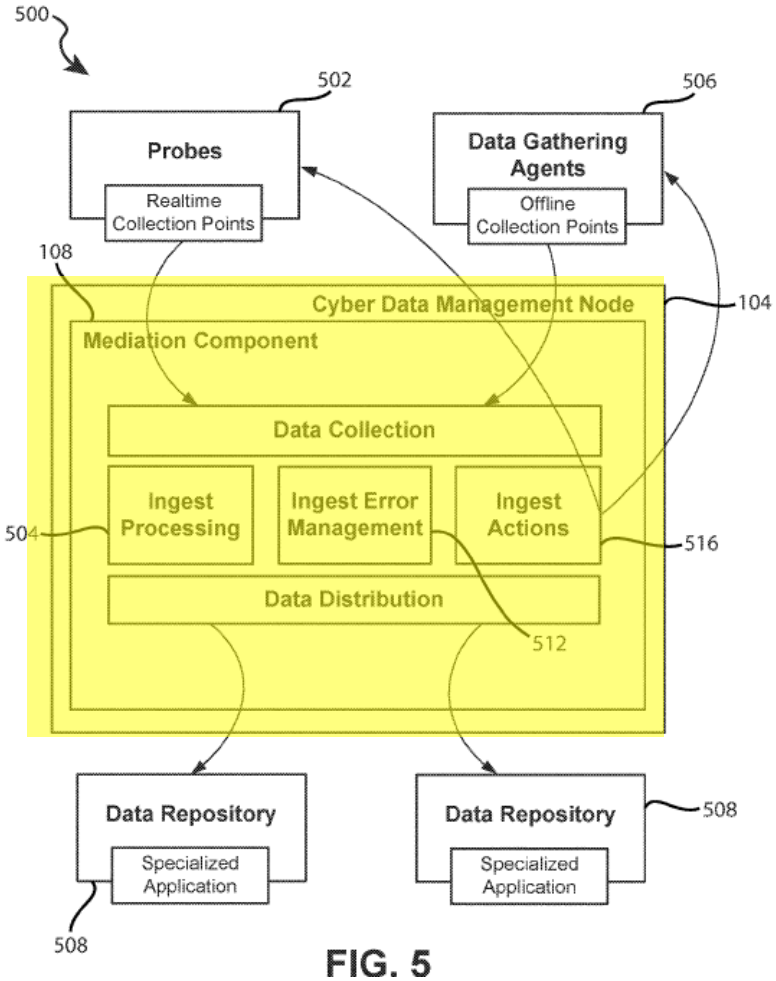
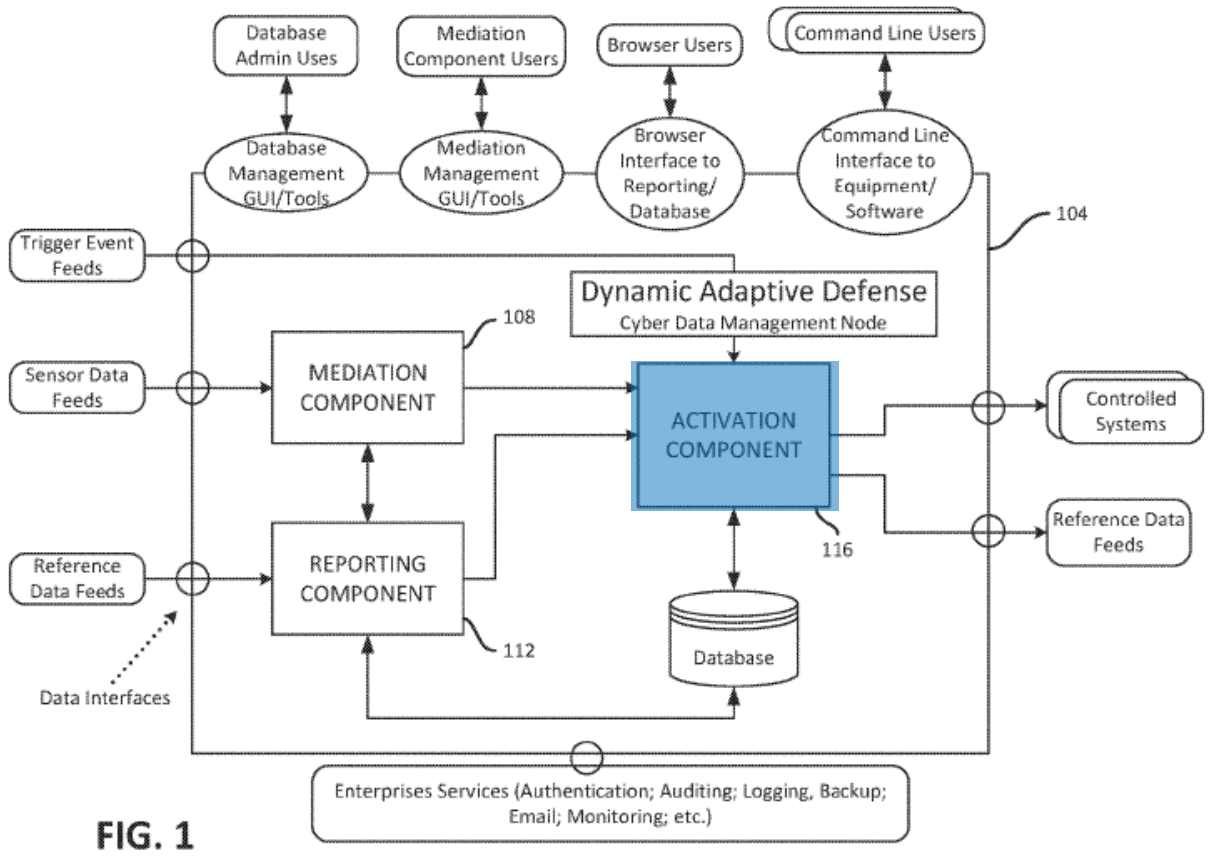


FIG. 5

Pet. 23-24 (citing EX-1004, FIG. 5; EX-1004, 8:13-21, 8:37-41, 8:49-53); *see also* Pet. 25-26 (citing EX-1004, FIG. 10 (identifying "DAD CDMN" element 104)). According to Petitioner "Thomas discloses a cyber-data management node (highlighted in yellow . . . in Figure 5), which acts as a SIEM. . . . Thus, the cyber-data management node serves as the SIEM of the claims." Pet. 23.

Regarding the "creating a work flow" limitation, Petitioner identifies and relies upon Thomas's cyber-data management node 104, and more specifically activation component 116, for disclosing that limitation. Pet. 22-30 (citing

EX-1004, Fig. 15A, 10, 14:21-23, 14:44-49, 15:4-12, 16:4-9, 20:4-6, 21:4-6, 22:10-18, 27:34-42). Activation component 116 (blue) is shown in Figure 1 of Thomas:



EX-1004, FIG. 1 (annotated). Petitioner contends:

> Thomas further discloses creating a workflow including a plurality of security tasks to be performed by one or more security devices. Ex. 1002, ¶ 117. Thomas describes that "[i]n responding to the cyber-security threat 728, the cyber-data management node 104 may initiate one or more automated workflows." Ex. 1004, 20:4–6. "These workflows may initiate an action directly." *Id.*,

14:21–23. The workflow includes "actions . . . or action plans which are specifically targeted towards security incident remediation. The nature of these systems varies according to the controlled environment, and may include (but not be limited to) devices such as firewalls, IPS (intrusion prevention systems), HBSS (host-based security systems), routers, and virus prevention systems." *Id.*, 15:4–12; Ex. 1002, ¶ 117. Thomas provides example actions such as "the configuration, activation, or deactivation of devices/applications to conduct actions, such as, surveillance, sniffers, network blocking, as well as activating new elements within the network." Ex. 1004, 14:44–49. Another example is "instructing a set of firewalls to block packets which match specific criteria which have been isolated from analysis of this specific attack. This set of instructions may be encoded as business logic within the activation component 116 and may include issuing a command to a device." *Id.*, 16:4–9. Another example is "removing an external user from directory service (operation 1220), reclassifying the external user in the directory service (operation 1222), and/or using an IPS to block inbound/outbound traffic (operation 1224)." *Id.*, 22:10–18; Ex. 1002, ¶ 118.

Thomas further explains that it can analyze the network data and "take[] any appropriate automated action that is indicated by the data aggregated in operation 1108 . . . without any specific human intervention." Ex. 1004,

> 21:4–6. Thus, the work flow may be created automatically by Thomas's cyber-data management node. Ex. 1002, ¶ 119.

Pet. 26-27.

Petitioner fails to meet its burden. None of the portions of Thomas that Petitioner identifies and relies upon disclose, teach, or suggest the "creating a work flow" limitation, as required by Claims 1 and 15. *See* EX-1004, FIG. 15A, FIG. 10, 14:21-23, 14:44-49, 15:4-12, 16:4-9, 20:4-6, 21:4-6, 22:10-18, 27:34-42.

Specifically, independent Claims 1 and 15 both require that the step of creating a work flow is performed by the SIEM device/system. EX-1001, 18:18-21 (requiring "creating, by a security information and event management (SIEM) device . . . a work flow") (Claim 1), 19:21-28 (requiring "the security information and event management (SIEM) system . . . perform a method comprising creating a work flow") (Claim 15). The '421 Patent further makes clear that the SIEM device "create[s] a work flow that includes multiple tasks." EX-1001, 1:52-54; *see also* EX-1001, 2:36-40 (disclosing the SIEM device "create[s] a work flow or work flow template"), 2:45-47 (disclosing the SIEM device "create[s] a work flow").

Yet, Petitioner does not identify any specific disclosure in Thomas that cyber-data management node 104 (the alleged SIEM device/system in Thomas) performs the required step of creating a work flow in the manner claimed. As noted above, the portions of Thomas that Petitioner relies upon and identifies as allegedly

disclosing the "creating a work flow" limitation, all describe or relate to Thomas's cyber-data management node 104—and namely the activation component 116—performing the functions of activating, executing, or initiating a work flow. *See, e.g.*, EX-1004, 14:21-23 (describing "initiat[ing] pre-configured workflows" and "[t]hese workflows may initiate an action"), 14:44-49 (describing a component that "provides an ability to initiate, the configuration, activation, or deactivation of devices/applications to conduct actions"), 20:4-6 (disclosing "the cyber-data management node 104 may then respond to the security threat 728 by initiating at least one automated action"). None of these relied-upon portions of Thomas discloses or suggests cyber-data management node 104, activation component 116, or any other of Thomas's components are actually **creating** a work flow, as required by Claims 1 and 15.

Moreover, Petitioner does not identify sufficient evidence or explain how or why a POSA would have understood Thomas's disclosures regarding activating, executing, and/or initiating a work flow as teaching or suggesting the "creating a work flow" limitation of the claims. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (requiring "reasoning with some rational underpinning to support the legal conclusion of obviousness"). Petitioner's assertions that "Thomas . . . discloses creating a workflow" and "the work flow may be created automatically by Thomas's

cyber-data management node" (Pet. 26-27) are conclusory and, without more, are insufficient to satisfy Petitioner's burden.

Because Thomas does not disclose the "creating a work flow" limitation, the Petition fails to demonstrate a reasonable likelihood that Challenged Claims 1 and 15 are unpatentable. Additionally, because the remaining Challenged Claims 4–10 and 18–24 ultimately depend from Claims 1 or 15, for at least the same reasons discussed above for Claims 1 and 15, the Petition fails to demonstrate a reasonable likelihood that Challenged Claims 4–10 and 18–24 are unpatentable.

VII. CONCLUSION

For the reasons set forth above, Patent Owner requests the Board deny institution of all grounds, and thus decline to institute *inter partes* review on any claim of the '421 Patent.

Dated: October 29, 2021

Respectfully submitted,

By: /Patrick D. McPherson/

Patrick D. McPherson,
Reg. No. 46,255
PDMcPherson@duanemorris.com
DUANE MORRIS LLP
505 9th St. NW, Suite 1000
Washington, D.C. 20004
P: (202) 776-5214
F: (202) 776-7801

Attorney for Patent Owner

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), the undersigned certifies that the forgoing document, excluding exempted portions, contains 4,708 words, which is less than the limit of 14,000 words set forth in 37 C.F.R. §§ 42.24(a)(1)(i) and 42.24(b)(1).

Dated: October 29, 2021

Respectfully submitted,

By: /Patrick D. McPherson/

Patrick D. McPherson,
Reg. No. 46,255
PDMcPherson@duanemorris.com
DUANE MORRIS LLP
505 9th St. NW, Suite 1000
Washington, D.C. 20004
P: (202) 776-5214
F: (202) 776-7801

Attorney for Patent Owner

CERTIFICATION OF SERVICE ON PETITIONER

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.107, the undersigned certifies that on the 29th day of October 2021, a complete and accurate copy of the foregoing Patent Owner's Preliminary Response and all supporting exhibits were served by filing this document with the Patent Review Processing System as well as via email to the following addresses:

Katherine A. Vidal (Reg. No. 46,333)
Louis L. Campbell (Reg. No. 59,963)
Matthew R. McCullough
James C. Lin
WINSTON & STRAWN LLP
275 Middlefield Rd, Suite 205
Menlo Park, California 94025
kvidal@winston.com
llcampbell@winston.com
mrmccullough@winston.com
jalin@winston.com
Winston-Forescout-Fortinet-IPRs@winston.com

Kimball R. Anderson
WINSTON & STRAWN LLP
35 W. Wacker Drive
Chicago, Illinois 60601
kanderso@winston.com
Winston-Forescout-Fortinet-IPRs@winston.com

Respectfully submitted,

By: /Patrick D. McPherson/

Patrick D. McPherson,
Reg. No. 46,255
PDMcPherson@duanemorris.com
DUANE MORRIS LLP
505 9th St. NW, Suite 1000
Washington, D.C. 20004
P: (202) 776-5214
F: (202) 776-7801

Attorney for Patent Owner