IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORESCOUT TECHNOLOGIES, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

Case No. IPR2021-01328
U.S. Patent No. 9,503,421

PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1, 4–10, 15, and 18–24 OF U.S. PATENT NO. 9,503,421

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PETITIONER'S EXHIBIT LIST

Ex. No.	Brief Description
1001	U.S. Patent No. 9,503,421 ("'421 patent")
1002	Declaration of Eric Cole, Ph.D.
1003	CV of Eric Cole, Ph.D.
1004	U.S. Patent No. 10,129,290 ("Thomas")
1005	U.S. Provisional App. No. 61/944,019 ("Thomas Provisional")
1006	U.S. Patent App. Pub. No. 2012/0224057 ("Gill")
1007	File History of U.S. Patent No. 9,503,421
1008	*Fortinet, Inc. v. Forescout Techs., Inc.*, No. 3:20-cv-03343-EMC (N.D. Cal. May 15, 2020), Amended Complaint (Document 67)
1009	*Fortinet, Inc. v. Forescout Techs., Inc.*, No. 3:20-cv-03343-EMC (N.D. Cal. May 15, 2020), Joint Claim Construction and Prehearing Statement (Patent Local Rule 4-3) (Document 90)
1010	*Trusted Knight Corp. v. Int'l Bus. Mach. Corp.*, No. 19-cv-01206-EMC (N.D. Cal. Aug. 31, 2020) (Document 112)
1011	*Robert Bosch Healthcare Sys. Inc. v. Cardiocom, LLC*, No. 14-cv-1575-EMC (N.D. Cal. July 3, 2014) (Document 145)

I. Introduction

Petitioner Forescout Technologies, Inc. ("Forescout") requests *inter partes* review of claims 1, 4–10, 15, and 18–24 of U.S. Patent No. 9,503,421 (the "'421 patent") (Ex. 1001) under 35 U.S.C. §§ 311–19 and 37 C.F.R. § 42.100 *et seq*.

Forescout asserts that there is a reasonable likelihood that the challenged claims are unpatentable and requests review and cancellation of claims 1, 4–10, 15, and 18–24 under 35 U.S.C. § 103.

II. Forescout Has Standing and the '421 Patent Is Eligible for *Inter Partes* Review.

Petitioner may file this petition. Forescout certifies pursuant to Rule 42.104(a) that the '421 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the identified grounds. Forescout was sued for alleged infringement of the '421 patent in the U.S. District Court for the Northern District of California by Patent Owner Fortinet, Inc. ("Fortinet") in an Amended Complaint filed and served on December 2, 2020. Ex. 1008.

III. Overview of the '421 patent

A. Subject Matter

The '421 patent is titled "Security Information and Event Management." Ex. 1001, Cover. The '421 patent identifies an alleged problem arising in conventional network security systems that "tasks that can be conducted by security devices of

the network are independent and results of such tasks cannot be transferred to another task. Furthermore, tasks conducted by different security devices may require different parameters. Even the same task may require different parameters when it is conducted by security devices from different manufacturers." *Id.*, 1:37–43. It thus identifies a "need for improved SIEM devices that may schedule multiple tasks of various security devices to automatically achieve comprehensive management." *Id.*, 1:43–46.

According to the '421 patent, its purported invention is "[s]ystems and methods . . . for conducting work flows by an SIEM device to carry out a complex task automatically." *Id.*, 1:50–52. To accomplish this, the '421 patent describes using "work flows." "A work flow defines a work flow task that contains a group of tasks that may be sequentially or concurrently conducted by one or more security devices so that a complex function may be accomplished automatically by SIEM device 200." *Id.*, 8:19–23.

An example of using the '421 patent's invention is shown below in Figure 3. In steps 301 and 302, the work flow is created from a template. In step 303, "the work flow is scheduled by the task scheduling engine." *Id.*, 12:53–54. In step 304, "execution results of tasks are collected by the task scheduling engine." *Id.*, 12:62–63. The results can be used to determine "if a following task should be triggered." *Id.*, 12:63–66. Finally, in step 305, "the task scheduling engine may also report the

execution results of the work flow to an administrator of the SIEM device." *Id.*, 13:4–6.

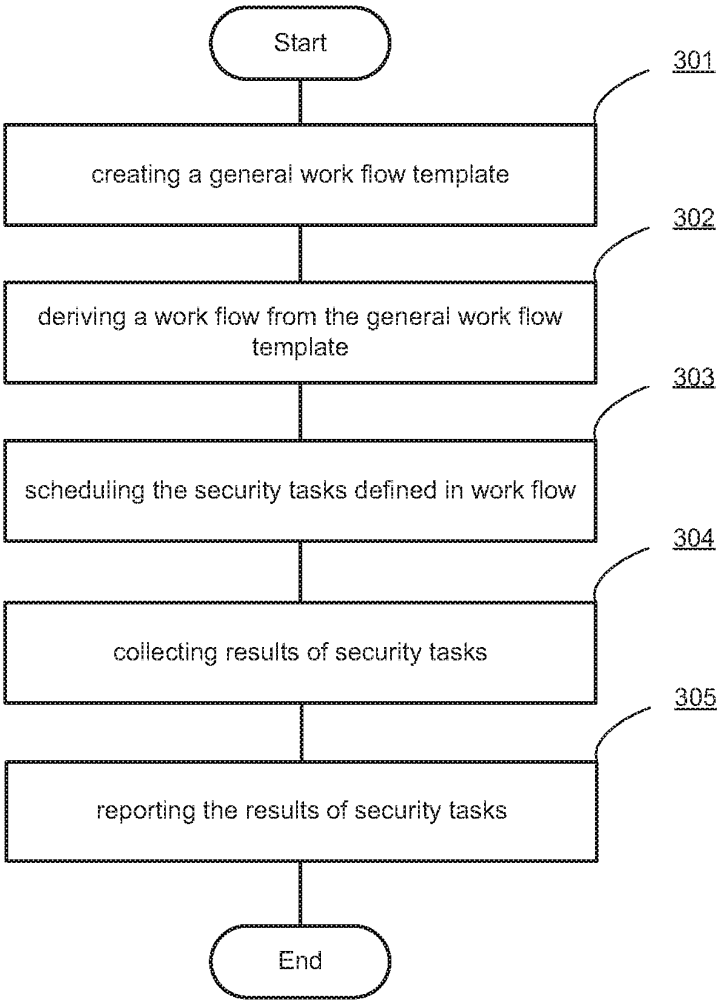


FIG. 3

B. Prosecution History

During prosecution, the examiner made a § 102 rejection based on U.S. Patent No. 9,069,930 ("Hart"). Ex. 1007 at 69–76. Applicant overcame the objection by amending the claims to recite that the security tasks are intended to protect the

private network against attacks, and distinguishing over Hart as merely disclosing "database query operations." *Id.* at 91–103. In response, the examiner issued a Notice of Allowance. *Id.* at 109–16.

None of the prior art cited in this petition was cited during prosecution, nor is it cumulative of anything cited during prosecution.

C. Effective Filing Date

The application for the '421 patent was filed on March 17, 2014. Ex. 1001, Cover. It does not claim the benefit of any earlier filing date. *Id.* For the purposes of this petition only, Petitioner assumes March 17, 2014 is the effective filing date of the '421 patent. The '421 patent is therefore subject to post-AIA rules.

D. Level of Ordinary Skill in the Art

As of March 17, 2014, a person of ordinary skill in the art ("POSITA") at the time of the '421 patent's effective filing date would typically be a person with a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields. Ex. 1002, ¶¶ 25–28. Someone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience, could also be considered a POSITA. *Id*. This level of skill in the art is reflected by the references

cited in this petition, the state of the art, and the experience of Dr. Eric Cole, as described in his declaration. In this petition, references to a POSITA refer to a person with these or similar qualifications.

IV. Claim Construction

The claim terms are to be construed under the same claim construction standard as civil actions in federal district court. 37 C.F.R. § 42.100(b).

In the litigation, the parties have agreed to the following constructions:

Term	Agreed Construction (Ex. 1009 at 1)
"in parallel"	"concurrently or simultaneously"
"serially"	"sequentially"

In the litigation, the parties have proposed the following competing constructions:

Term	Patent Owner Construction (Ex. 1009 at 20–25)	Petitioner Construction (Ex. 1009 at 20–25)
"a work flow"	"a set of security tasks and related logical conditions relating to said security tasks, where said security	"data that defines a work flow task that contains a group of tasks that may be sequentially

	tasks comprise more than only database queries"	or concurrently conducted by one or more security devices"
"security information and event management (SIEM) [device]"	"hardware device that receives security and event information from security devices"	"a device that collects logs of security events from external sources for the purposes of identifying problems and/or threats, and/or to fulfill a regulatory requirement"

Additionally, Patent Owner has proposed the following constructions for terms where Petitioner has proposed plain and ordinary meaning or has proposed that the claim is indefinite.[1]

Term	Patent Owner Construction (Ex. 1009 at 20–25)
"core network assets"	"all or a subset of assets of the network designated by the administrator"

[1] As indefiniteness arguments may not be made in an IPR, Petitioner has applied Patent Owner's constructions of these terms in this petition. Petitioner reserves all right with respect to the litigation.

"normalizing the results"	"transforming the results such that information from the results may be retained and saved in a unified format"
"security device"	"device deployed to regulate network access and protect the network from attacks"
"security task"	"a task performed by a hardware device which is intended to protect a private network against attacks"

Forescout does not believe any of these terms require construction for this petition, as their construction would not affect the outcome of any trial on this petition. For the reasons explained below, the prior art invalidates even assuming these constructions apply.

V. Precise Relief Requested

A. Proposed Grounds and Prior Art

Pursuant to Rules 42.22(a)(1) and 42.104(b), the following grounds for trial are presented herein:

Ground 1: Claims 1, 4–10, 15, and 18–24 are obvious under 35 U.S.C. § 103 over U.S. Patent No. 10,129,290 to Thomas ("Thomas") (Ex. 1004) in view of the knowledge of a POSITA.

Ground 2: Claims 4–8 and 18–22 are obvious under 35 U.S.C. § 103 over Thomas in view of U.S. Patent App. Pub. No. 2012/0224057 to Gill ("Gill") (Ex. 1006).

The references relied upon in Grounds 1 and 2 are prior art.

Thomas is prior art under post-AIA 35 U.S.C. § 102(a)(2) because its effective filing date is at least as early as February 24, 2014, the filing date of U.S. Provisional App. No. 61/944,019 ("Thomas Provisional" (Ex. 1005)), which precedes the effective filing date of the '421 patent. Ex. 1004, Cover.[2] Although a priority analysis is not required under the AIA, the analysis showing Thomas is entitled to claim that priority date is below in Section VI.A.2.

Gill is prior art under at least post-AIA 35 U.S.C. §§ 102(a)(1) and (2) because it is a patent application that was published on September 6, 2012, before the '421 patent's effective filing date. Ex. 1006, Cover.

[2] There are additional earlier provisional applications that Thomas claims priority to, but for simplicity's sake, Petitioner has focused on this particular provisional, which is indisputably filed earlier than the earliest effective filing date of the '421 patent (March 17, 2014).

B. The Proposed Grounds Are Not Cumulative or Redundant.

The grounds for trial presented in this petition are not redundant of issues already examined during prosecution of the '421 patent. None of the prior art cited in this petition was cited during prosecution. Ex. 1001, Cover; *see generally* Ex. 1007 at 69–76, 91–103, 109–16 (specifically discussing only Hart).

VI. Detailed Explanation of Grounds for Institution

As proven below, claims 1, 4–10, 15, and 18–24 are unpatentable under 35 U.S.C. § 103. The claims, as a whole, would have been obvious to a POSITA under § 103 because, as shown below, every element of the claims was taught by the prior art. There is also nothing about any of the claims, as a whole, that would have made them non-obvious even though every element was taught in the prior art. Ex. 1002, ¶ 72.

A. Ground 1: Thomas Renders Claims 1, 4–10, 15, and 18–24 Obvious.

Claims 1, 4–10, 15, and 18–24 are invalid under 35 U.S.C. § 103 over Thomas. For the reasons explained below, a POSITA considering the teachings of this reference would have found the claimed subject matter obvious. Indeed, a POSITA would recognize that Thomas teaches all limitations of the claims and thus would render the claims obvious. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1373 (Fed. Cir. 2019) ("it is well settled that 'a disclosure that anticipates under

§ 102 also renders the claim invalid under § 103, for "anticipation is the epitome of obviousness."""").

1. Summary of Thomas

U.S. Patent No. 10,129,290 to Thomas et al. ("Thomas") is titled "Dynamic Adaptive Defense for Cyber-Security Threats." Ex.1004, Cover. Thomas describes "a cyber-security system that is configured to aggregate and unify data from multiple components and platforms on a network. The system allows security administrators to design and implement a workflow of device-actions taken by security individuals in response to a security incident." *Id.*, Abstract.

Thomas discloses a cyber-data management node, highlighted in yellow below in Figure 5:

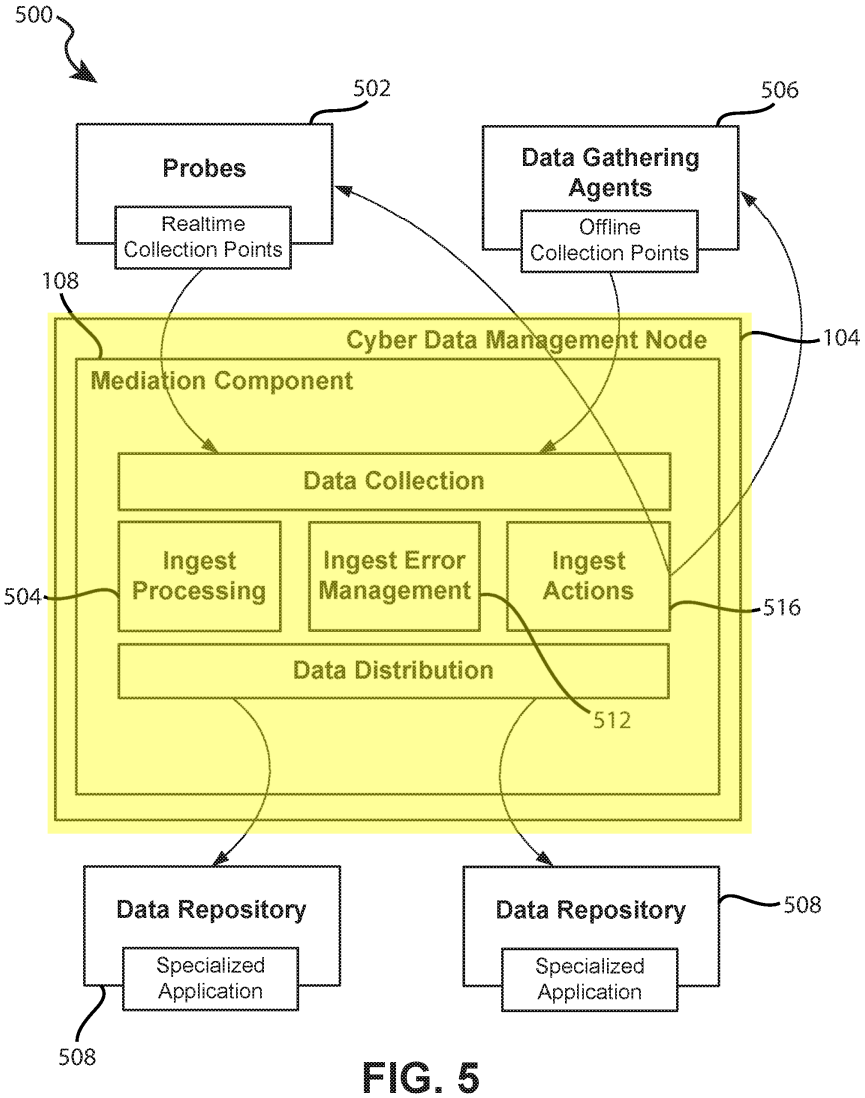
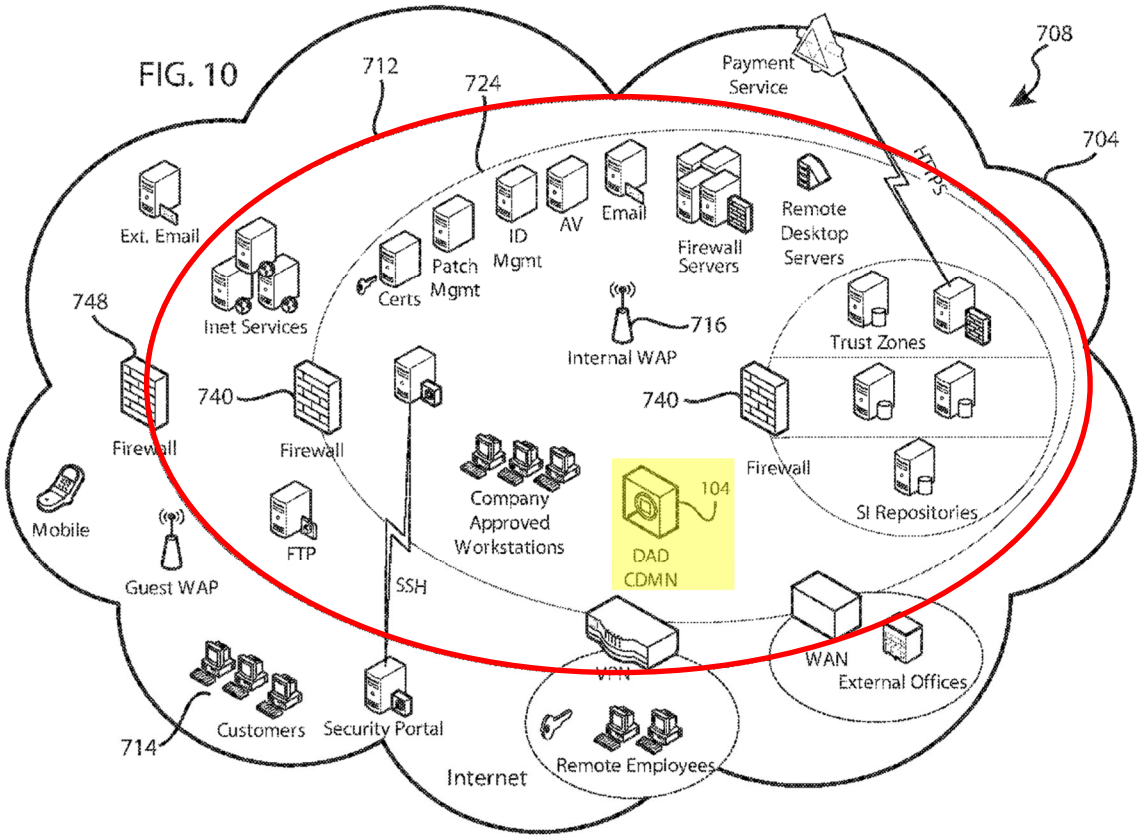


FIG. 5

Thomas teaches that the "cyber-data management node 104 node is generally configured to ingest internet protocol (IP) and other data for analysis to determine acceptance/denial in the network as well as dealing with disparate data and transforming it into an understandable and meaningful database for logical analysis. The cyber-data management node 104 includes a mediation component 108 that is configured to ingest, enrich, and analyze data regarding cyber-security alerts and threats." Ex. 1004, 8:13–21; Ex. 1002, ¶¶ 54–55.

Thomas's cyber-data management node is associated with a private network, such as an internal corporate network. *Id.*, ¶ 56. For example, Thomas depicts an example network in Figure 10 below. *Id.* Thomas teaches that "[t]he enterprise perimeter 712 separates the enterprise 708 from external networks such as the Internet 704." Ex. 1004, 19:26–28. As shown in Figure 10, the cyber-data management node (highlighted in yellow) is inside the enterprise perimeter 712 (red oval). Ex. 1002, ¶ 57.



Thomas further discloses creating a workflow including a plurality of security tasks to be performed by one or more security devices. Ex. 1002, ¶ 58. 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. 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, ¶ 58.

The actions can be visually depicted in Thomas's system, as shown below in Figure 15A. *Id.*, ¶ 59. As Thomas explains, "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. The various groups can be displayed in an order in which they [sic] to run. 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." Ex. 1004, 27:34–42. An example of two actions that run in parallel is highlighted in green below, and an example of two actions running in sequence is highlighted in blue. Ex. 1002, ¶¶ 60–61.

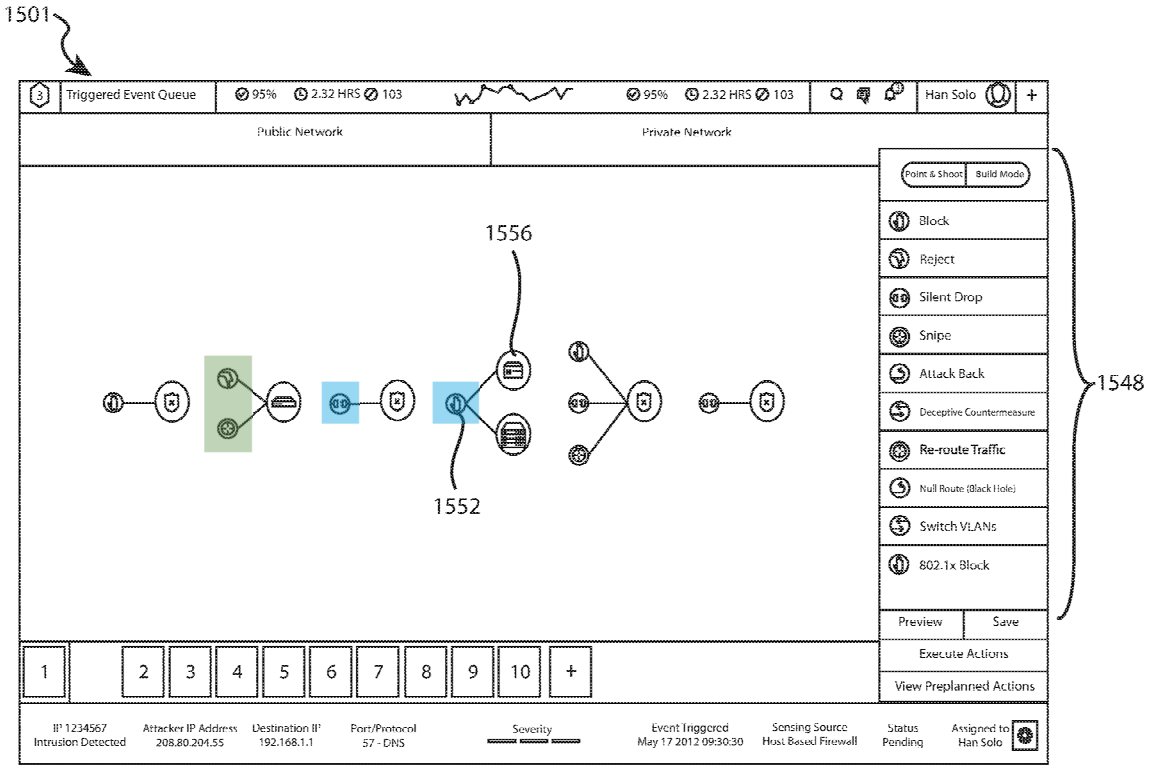


FIG. 15A

2. Thomas Is Prior Art

Thomas is prior art.

According to the Patent Office Manual of Patent Examining Procedure, under the AIA, "there is no need to evaluate whether any claim of a U.S. patent document is actually entitled to priority or benefit under 35 U.S.C. 119, 120, 121, 365, or 386 when applying such a document as prior art." MPEP § 2154.01(b) (9th ed. June 2020). Accordingly, 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 (Messrs. Thomas and Scott). *See id.*

Although 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. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (under pre-AIA rules, prior art reference is entitled to claim priority to date of provisional application if provisional contains written description support of claim in the prior art reference).[3]

Specifically, Dr. Cole's analysis shows that the Thomas Provisional provides written description and enablement support for at least claim 11 of Thomas. Ex. 1002, ¶¶ 73–104.

Limitation [11pre] of Thomas recites "A system for responding to a cyber-security attack, comprising." Ex. 1004, 35:8–9. The Thomas Provisional discloses

[3] Although *Dynamic Drinkware* was a pre-AIA case, the Board has applied *Dynamic Drinkware* to certain post-AIA cases. *See, e.g.*, *Mueller Sys., LLC v. Rein Tech, Inc.*, Case No. IPR2020-00100, 2020 WL 2478524, at *10 (PTAB May 12, 2020); *Found. Med., Inc. v. Guardant Health, Inc.*, Case No. IPR2019-00652, 2019 WL 3928929, at *7–8 (PTAB Aug. 19, 2019); *Westinghouse Air Brake Techs. Corp. v. Siemens Mobility, Inc.*, Case No. IPR2017-00580, 2019 WL 164710, at *10–12 (PTAB Jan. 10, 2019); *Epizyme, Inc. v. GlaxoSmithKline LLC*, Case No. IPR2020-01577, 2021 WL 841118, at *10–11 (PTAB Mar. 5, 2021).

a "distributed denial of service (DDoS) detection and reaction solution . . . to provide visibility into network behavior, alert analysts to anomalous events and provide mitigation options to attacks. The solution provides a dynamic active defense (DAD) capable of receiving an indication of cyber threat and executing defined actions in an automated manner (with or without human intervention) to address that threat." Ex. 1005, ¶ [0004]. *See also id.*, ¶¶ [0008] ("Present embodiments are directed to a cyber-security system that is configured to aggregate and mediate data from multiple components and platforms on a network. Based on the nature of a particular threat, the cyber-security system may initiate a workflow that automates a response tailored to the threat to protect potentially impacted components and network resources."), [0059] ("It also provides the foundation for responding in real time to advanced persistent threats"); Ex. 1002, ¶¶ 77–79.

Limitation [11a] of Thomas recites "at least one processor." Ex. 1004, 35:10. The Thomas Provisional discloses "the computer system 300 includes a processor 302." Ex. 1005, ¶ [0012]; Ex. 1002, ¶¶ 80–82.

Limitation [11b] of Thomas recites "at least one memory operably linked to the at least one processor, the at least one memory including instructions, which when executed on the at least one processor, cause the processor to." Ex. 1004, 35:11–14. The Thomas Provisional discloses "a hard disk drive 318 for nonvolatile storage of applications, files, and data." Ex. 1005, ¶ [0013]. It further teaches "the

hard disk drive may store code associated with the cyber-data management node 104 according to the exemplary processes described herein." *Id.* As explained below, the Thomas Provisional teaches that the cyber-data management node performs the recited steps. Ex. 1002, ¶¶ 83–86.

Limitation [11b1] of Thomas recites "display a plurality of network security element icons in a network security map." Ex. 1004, 35:15–16. The Thomas Provisional describes "an exemplary interactive network map 700." Ex. 1005, ¶ [0062]. This map "may include a network diagram 716 that represents the monitored network 800 broken out by elements that can be controlled in responding to a security threat." *Id.*, ¶ [0063]. An example network map is shown in Figure 7A.[4] Ex. 1002, ¶¶ 87–89.

[4] Although the figures in the Thomas Provisional are difficult to read, they can be understood based on the specification of the Thomas Provisional. Additionally, the same drawings are present as Figure 15 in Thomas and in its priority application, which was published as WO2015051181A1.

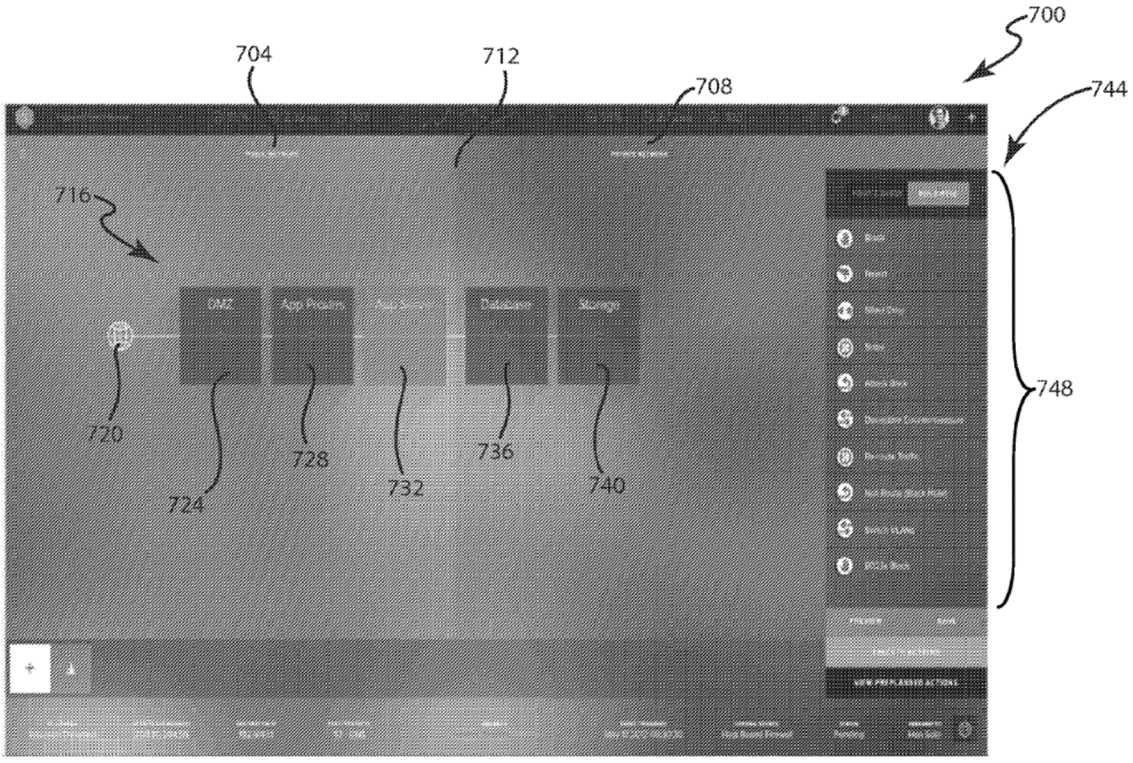


FIG. 7A

Thomas further depicts that the map can show individual security elements such as FW (firewall) and IDS (intrusion detection system) in Figure 7E below. *Id.*, ¶¶ 90–91. A POSITA would understand that firewalls and IDS are well-known network security elements. *Id.*

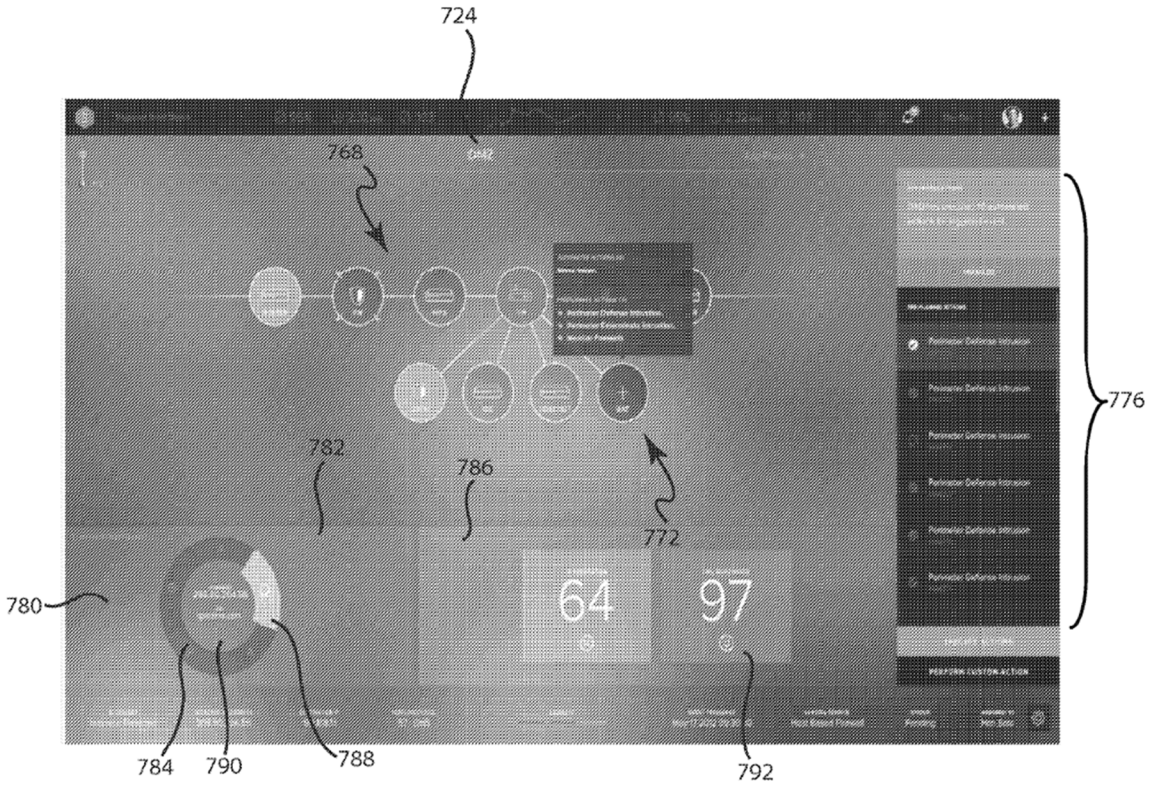


FIG. 7E

Limitation [11b2] of Thomas recites "display a plurality of cyber-security countermeasure icons in the network security map." Ex. 1004, 35:17–18. The Thomas Provisional teaches that the map "may also contain a menu 744 having a number of drag and drop items 748. The drag and drop items 748 may be selected and moved to particular network elements so as to initiate certain preplanned actions." Ex. 1005, ¶ [0064]. The Thomas Provisional further provides an example of the "common-English action names (like 'Block')" that may be performed. *Id.*, ¶ [0065]. A POSITA would understand "Block" is an exemplary security countermeasure. Ex. 1002, ¶¶ 92–94. The Thomas Provisional further teaches that "[t]he pre-planned action display 776 may include actions or groups of actions that,

as part of an approved cyber-security policy, are associated with certain types of cyber-security threats." Ex. 1005, ¶ [0068]; Ex. 1002, ¶¶ 95–96.

Limitation [11b3] of Thomas recites "receive a user input that correlates at least one network security element icon from the plurality of the network security elements icons with at least one cyber-security countermeasure icon from the plurality of the cyber-security countermeasure icons, the at least one network security element icon lacking correlations in the network security map with the at least one cyber-security countermeasure icon prior to receiving the user input." Ex. 1004, 35:19–27. As the Thomas Provisional states, "[t]he drag and drop items 748 may be selected and moved to particular network elements so as to initiate certain preplanned actions. Fig. 7B shows several actions 752 being associated with network elements 756." Ex. 1005, ¶ [0064]. As described above, an exemplary action is "Block." *Id.*, ¶ [0065]. Thus, a user may associate a countermeasure like "Block" with a network security element by dragging and dropping on the map. "[T]he visible security elements can be dragged onto dedicated area 760 or other assembly stage, grouped with common-English action names (like 'Block'), saved, and executed." *Id.* The user may drag and drop this onto an element not already having a "Block" action correlated with it, thus meeting the limitation. Ex. 1002, ¶¶ 97–99.

Limitation [11b4] of Thomas recites "send a signal to apply a cyber-security countermeasure to a network security element responsive to the user input, the cyber-security countermeasure corresponding to the at least one cyber-security countermeasure icon, the network security element corresponding to the at least one network security element icon." Ex. 1004, 35:28–34. The Thomas Provisional states that "[t]he drag and drop items 748 may be selected and moved to particular network elements so as to initiate certain preplanned actions. Fig. 7B shows several actions 752 being associated with network elements 756." Ex. 1005, ¶ [0064]. As described above, an exemplary action is "Block." *Id.*, ¶ [0065]. Thus, if a user drags and drops the "Block" action to a network security element, the Thomas Provisional explains that the system will cause the particular network element to "initiate" the action. *Id.*, ¶ [0064]; Ex. 1002, ¶¶ 100–02.

Thus, each and every limitation of claim 11 of Thomas is supported by the Thomas Provisional (Ex. 1002, ¶ 103), and Thomas is therefore entitled to claim prior art to the filing date of the Thomas Provisional under *Dynamic Drinkware*.

Because 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 under 35 U.S.C. § 102(a)(2). Thomas and the '421 patent do not share any common inventors or assignees, and Fortinet has not alleged that any exception in 35 U.S.C. § 102(b) applies. Thus, Thomas is prior art.

3. Claim 1

Claim 1 would have been obvious under 35 U.S.C. § 103 over Thomas. Ex. 1002, ¶ 105.

a. [1pre] "A method comprising:"

To the extent this preamble is a limitation, Thomas discloses a method. Ex. 1002, ¶¶ 106–08. For example, Thomas describes "a cyber-security system that is configured to aggregate and unify data from multiple components and platforms on a network." Ex. 1004, Abstract. This system performs methods such as "implement[ing] a workflow of device-actions taken by security individuals in response to a security incident" and "initiat[ing] an action plan that is tailored to the security operations center and their operating procedures to protect potentially impacted components and network resources." *Id.*; Ex. 1002, ¶ 107.

b. [1a] "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 protect the private network against attacks;"

Thomas discloses this limitation. Ex. 1002, ¶¶ 109–27.

Thomas discloses a cyber-data management node (highlighted in yellow below in Figure 5), which acts as a SIEM.[5] Thomas makes clear that the cyber-data management node provides augmented or enhanced SIEM functionality. Ex. 1004, 8:49–53 ("By automating or partially automating determinative analytics and/or system controls, a cyber-data management node 104 can enhance or augment SIEM solutions.") Thus, the cyber-data management node serves as the SIEM of the claims. Ex. 1002, ¶¶ 110–11.

[5] Thomas also states that the cyber-data management node may optionally "be deployed in conjunction with a security incident and event manager ('SIEM')." Ex. 1004, 8:37–41. But this optional SIEM is not required and the cyber-data management node itself can serve as the SIEM.

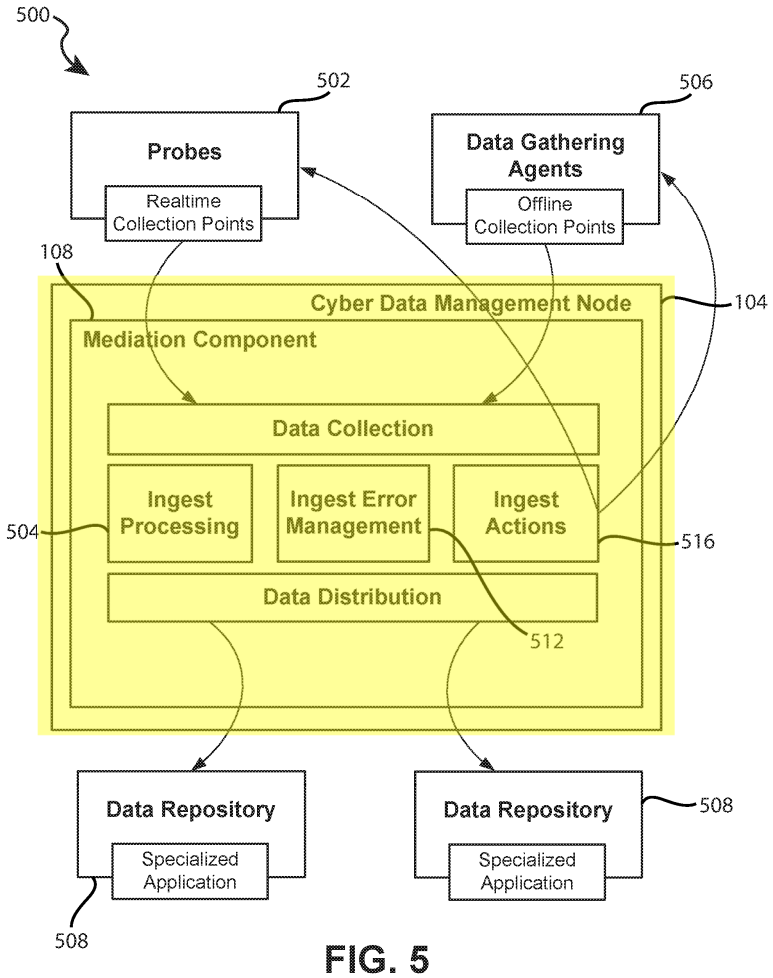


FIG. 5

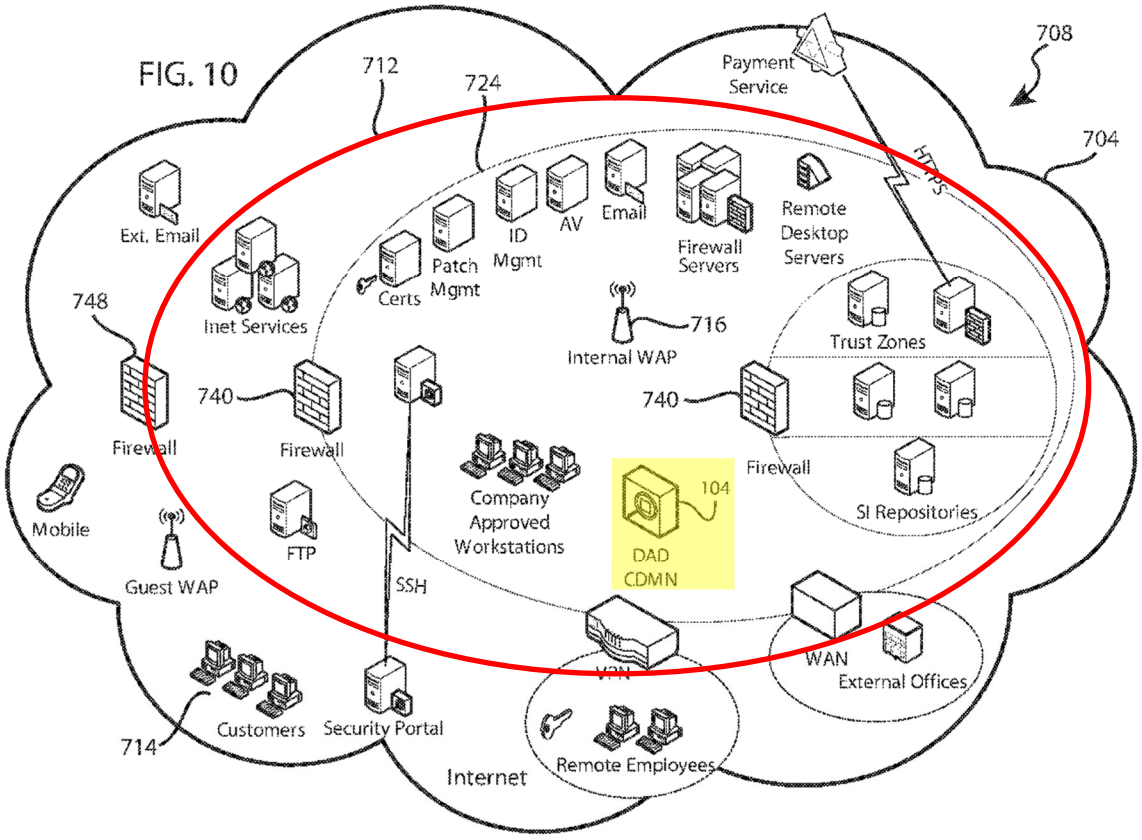
Thomas teaches that the "cyber-data management node 104 node is generally configured to ingest internet protocol (IP) and other data for analysis to determine acceptance/denial in the network as well as dealing with disparate data and transforming it into an understandable and meaningful database for logical analysis. The cyber-data management node 104 includes a mediation component 108 that is configured to ingest, enrich, and analyze data regarding cyber-security alerts and threats." Ex. 1004, 8:13–21. The information ingested by the cyber-data management node may include probe data, which may include "firewall logs." *Id.*,

18:33–42. The cyber-data management node is implemented on "computer system 300," which may be a "single server" or "other computer devices." *Id.*, 8:59–9:1. Ex. 1002, ¶ 112.

Thomas meets both parties' proposed constructions of "security information and event management (SIEM) device." Ex. 1002, ¶ 113–15. Patent Owner's construction of "hardware device that receives security and event information from security devices" (Ex. 1009 at 24) is satisfied because Thomas teaches that the cyber-data management node is a hardware device that receives security and event information (e.g., cyber-security alerts) from security devices (e.g., firewalls). Ex. 1002, ¶ 114. Petitioner's construction of "a device that collects logs of security events from external sources for the purposes of identifying problems and/or threats, and/or to fulfill a regulatory requirement" (Ex. 1009 at 24) is satisfied because, as noted above, the cyber-data management node may collect logs from external sources (e.g., firewall logs) for the purposes of identifying problems and/or threats. Ex. 1002, ¶ 115.

Thomas's cyber-data management node, which acts as the SIEM, is associated with a private network, such as an internal corporate network. *Id.*, ¶ 116. For example, Thomas depicts an example network in Figure 10 below. Thomas teaches that "[t]he enterprise perimeter 712 separates the enterprise 708 from external networks such as the Internet 704." Ex. 1004, 19:26–28. As shown in Figure 10,

the cyber-data management node (highlighted in yellow) is inside the enterprise perimeter 712 (red oval), and is thus associated with the (private) enterprise network. Ex. 1002, ¶ 116.



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.

The actions can be visually depicted in Thomas's system, as shown below in Figure 15A. Ex. 1002, ¶ 120. As Thomas explains, "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. The various groups can be displayed in an order in which they [sic] to run. 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." Ex. 1004, 27:34–42. An example of two actions that run in parallel is highlighted in green below, and an example of two actions running in sequence (from left to right) is highlighted in blue. Ex. 1002, ¶ 121.

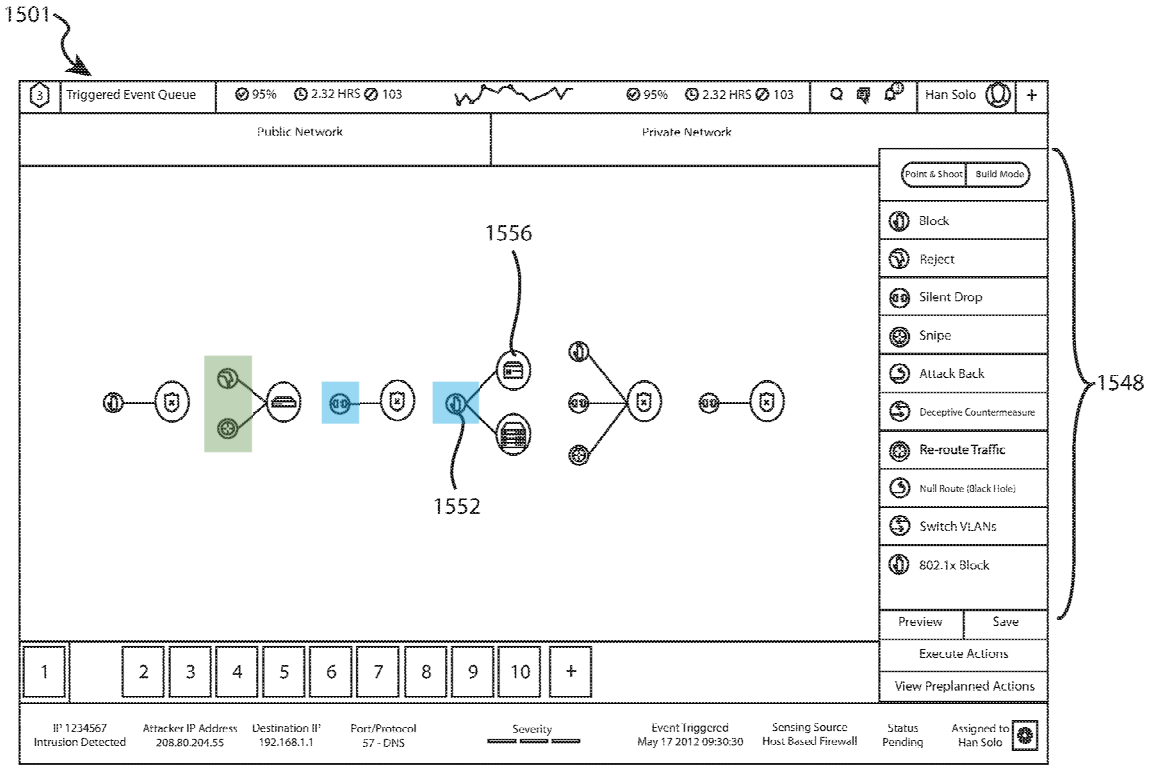


FIG. 15A

Thomas meets both parties' proposed constructions of "a work flow." Ex. 1002, ¶¶ 122–24. Patent Owner's construction of "a set of security tasks and related logical conditions relating to said security tasks, where said security tasks comprise more than only database queries" (Ex. 1009 at 20) is satisfied because Thomas discloses that the workflow includes security tasks that are more than database queries (e.g., blocking packets on a firewall) and related logical conditions (e.g., business logic). Ex. 1002, ¶ 123. Petitioner's construction of "data that defines a work flow task that contains a group of tasks that may be sequentially or concurrently conducted by one or more security devices" (Ex. 1009 at 20) is satisfied because Thomas explains the work flow may contain a group of actions that can be

performed by one or more devices, which, as shown in Figure 15A above, may run in sequence or concurrently. Ex. 1002, ¶ 124.

Thomas meets Patent Owner's construction of "security task" as "a task performed by a hardware device which is intended to protect a private network against attacks." Ex. 1009 at 25. For example, Thomas provides the specific examples of "surveillance," "network blocking," "block[ing] packets" on a firewall, and "using an IPS to block inbound/outbound traffic." All of these qualify as security tasks. A POSITA would understand these tasks are performed by hardware devices (e.g., a firewall or an IPS) on the network and are intended to protect a private network against attacks. Ex. 1002, ¶ 125.

Thomas meets Patent Owner's construction of "security device" as "device deployed to regulate network access and protect the network from attacks." Ex. 1009 at 23. For example, Thomas discloses a "firewall" and "IPS" (intrusion prevention system), which are both well-known devices that regulate network access. Also, as depicted in Figure 10 above, other security devices can be used in Thomas's system, including "Remote Desktop Servers" and "VPN," both of which are other examples of devices that regulate access to a network (e.g., from a remote location). Ex. 1002, ¶ 126.

c. [1b] "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"

Thomas discloses this limitation. Ex. 1002, ¶¶ 128–33.

Thomas discloses that the cyber-data management node, which acts as the SIEM, includes an "activation component," as shown in Figure 4 below. Ex. 1002, ¶ 129. The activation component "is configured to respond to manual triggers and/or triggers received from the mediation component 108 by controlling and/or managing disparate network elements to mitigate cyber-security threats." Ex. 1004, 14:27–33. "The use of an activation component 116 in a given implementation, such as an overall DDoS solution architecture, provides an ability to initiate 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." *Id.*, 14:44–49; Ex. 1002, ¶ 130.

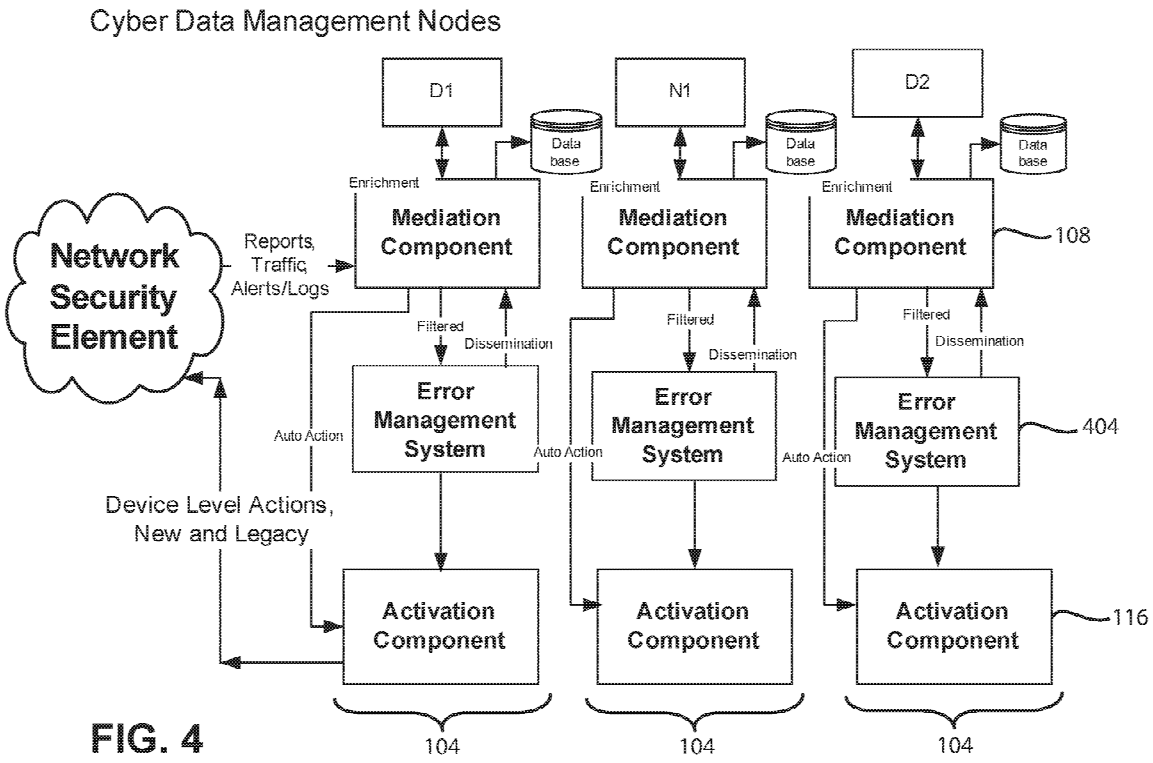


FIG. 4

Thus, the activation components starts or schedules the plurality of security tasks. Ex. 1002, ¶ 131. Additionally, as shown in Figure 15A, the tasks may be a sequence of actions, and thus the activation component schedules multiple tasks, some to occur in parallel (green highlighting) and others to occur in sequence (blue highlighting). *Id.*, ¶ 132.

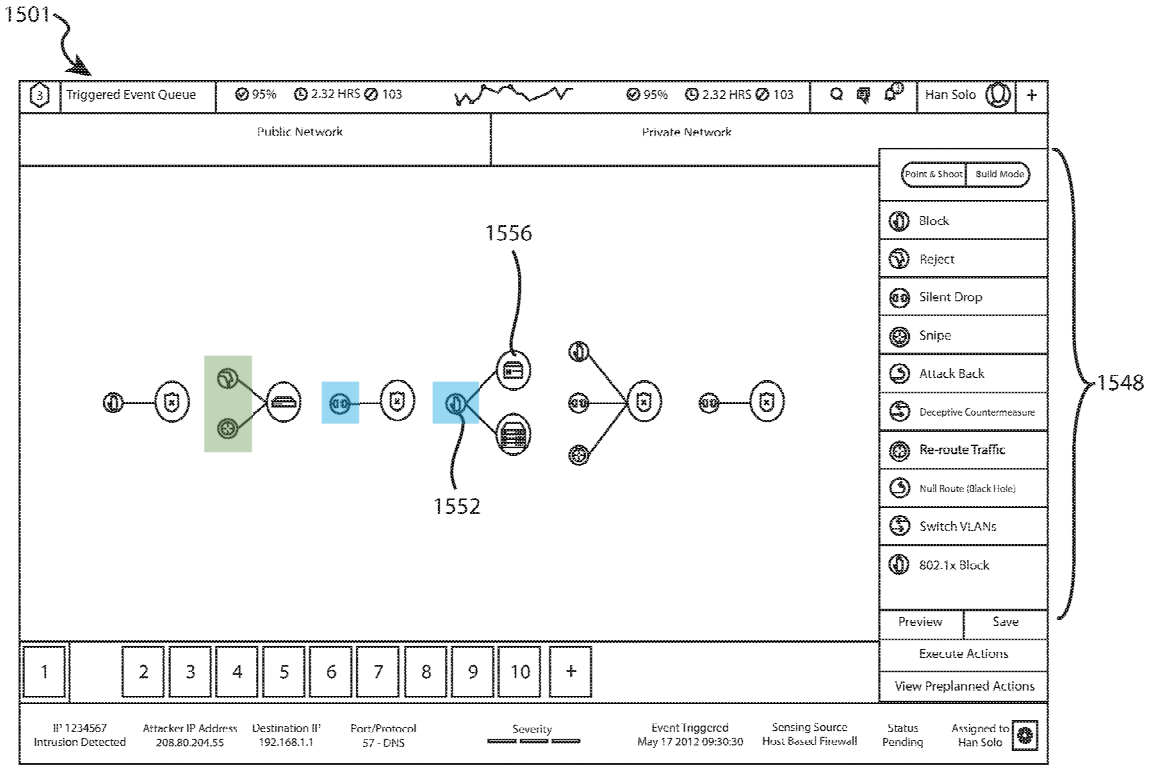


FIG. 15A

d. [1c] "collecting, by the SIEM device, results of the plurality of security tasks after they are performed by the one or more security devices."

Thomas discloses this limitation. Ex. 1002, ¶¶ 134–37.

Thomas discloses that "[t]he activation component 116 may provide diagnostic trace information which can show to the analyst individual device interactions if appropriate. The activation component 116 may additionally provide a summary interface identifying which devices were successfully affected, or which failed in the attempt." Ex. 1004, 16:15–19. Thus, Thomas discloses that the cyber-data management node, acting as the SIEM, collects results of security tasks (e.g., success or failure). Ex. 1002, ¶ 135. Additionally, as shown below in Figure 4, the

cyber-data management node operates in a cycle, with the mediation component of the cyber-data management node receiving "Reports, Traffic, Alerts/Logs" from the "Network Security Element" (on which actions are performed). Thus, the mediation component would receive reports or alerts after an action is performed, thereby further collecting any results from the actions performed by the one or more security devices. *Id.*, ¶ 136.

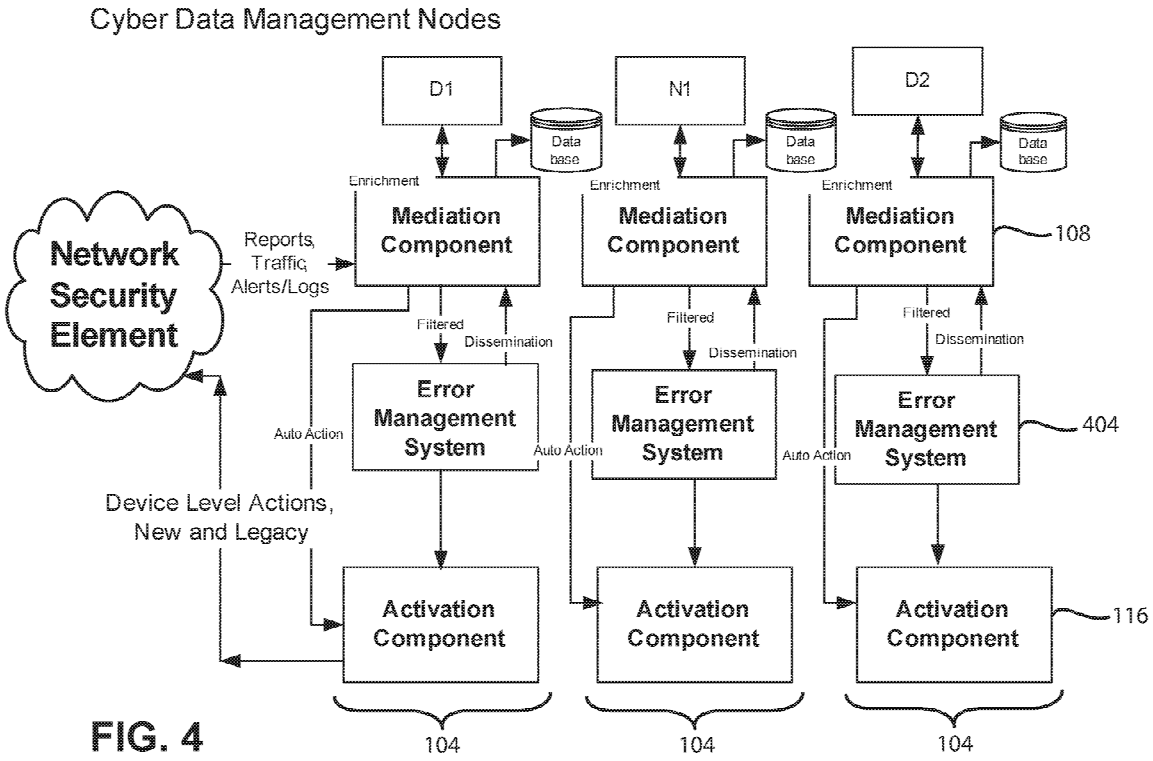


FIG. 4

A POSITA would therefore understand that Thomas discloses each limitation of claim 1 and thus renders it obvious. Ex. 1002, ¶¶ 105–37.

4. Claim 4

Claim 4, which depends from claim 1, further recites "wherein the plurality of security tasks of the work flow are performed serially." Ex. 1001, 18:47–48. This

additional element of claim 4 would have been obvious over Thomas. Ex. 1002, ¶¶ 138–42.

As described above, Thomas explains that actions can be performed in "parallel" or in "an order in which they [are] to run." Ex. 1004, 27:34–40. "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." *Id.*, 27:40–42. An example of two actions that run in sequence from left to right is highlighted in blue below in Figure 15A. Ex. 1002, ¶ 140.

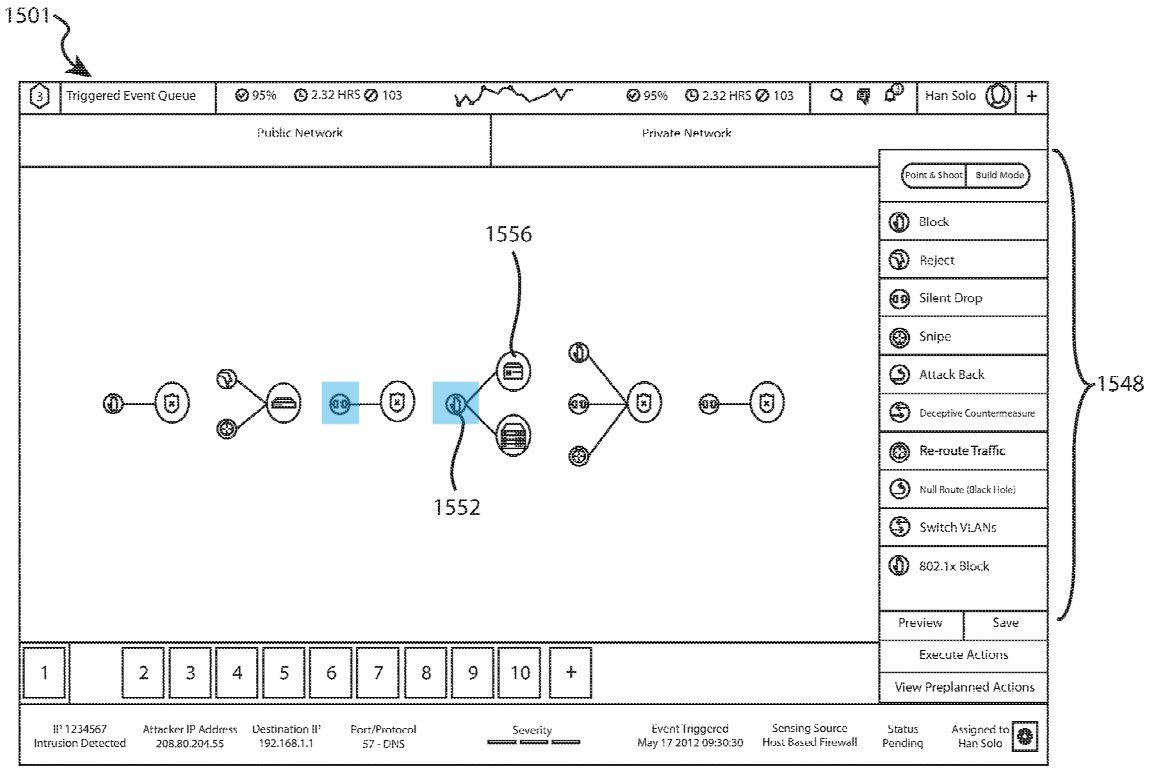


FIG. 15A

Thomas meets the parties' agreed construction of "serially," which is "sequentially." Ex. 1009 at 1. Thomas expressly describes Figure 15A as a

"sequencing diagram" that can show actions to be performed in a particular order (i.e., sequentially). Ex. 1002, ¶ 141.

5. Claim 5

Claim 5, which depends from claim 4, further recites "determining if a security task of the plurality of security tasks in the work flow should be performed based on the results of one or more previous security tasks of the plurality of security tasks of the work flow." Ex. 1001, 18:49–53. This additional element of claim 5 would have been obvious over Thomas. Ex. 1002, ¶¶ 143–47.

Thomas provides an example of the operation of the cyber-data management node in which an "initial set of search parameters may contain information related to a security alert received at the cyber-data management node 104." Ex. 1004, 22:44–46. The "mediation component 108 performs a search on the first or initial set of search parameters." *Id.*, 22:55–57. If additional data is needed, "[t]he mediation component 108 may achieve this result using a fluid process for saving and passing results of one search to the next search in order to provide context to what the next search may be querying on." *Id.*, 23:8–23. As shown in this example, Thomas's cyber-data management node (which is a SIEM) can determine whether to perform further actions (e.g., further searches relating to a security alert) based on the results of the previous actions (e.g., previous searches showing that additional data is needed relating to the security alert). Ex. 1002, ¶¶ 145–46.

6. Claim 6

Claim 6, which depends from claim 4, further recites "transferring results of one or more previous security tasks of the plurality of security tasks of the work flow to a next security task of the plurality of security tasks of the work flow." Ex. 1001, 18:54–57. This additional element of claim 6 would have been obvious over Thomas. Ex. 1002, ¶¶ 148–51.

As described above for claim 5, Thomas provides an example where, if additional data is needed, "[t]he mediation component 108 may achieve this result using a fluid process for saving and passing results of one search to the next search in order to provide context to what the next search may be querying on." Ex. 1004, 23:20–23. Thus, Thomas teaches providing results from one task (e.g., the prior search) to another (e.g., the next search). Ex. 1002, ¶ 150.

7. Claim 7

Claim 7, which depends from claim 1, further recites "wherein the plurality of security tasks of the work flow are performed in parallel." Ex. 1001, 18:58–59. This additional element of claim 7 would have been obvious over Thomas. Ex. 1002, ¶¶ 152–56.

As described above, Thomas explains that actions can be performed in "parallel" or in "an order in which they [are] to run." Ex. 1004, 27:34–40. An

example of two actions that run in parallel is highlighted in green below in Figure 15A. Ex. 1002, ¶ 154.

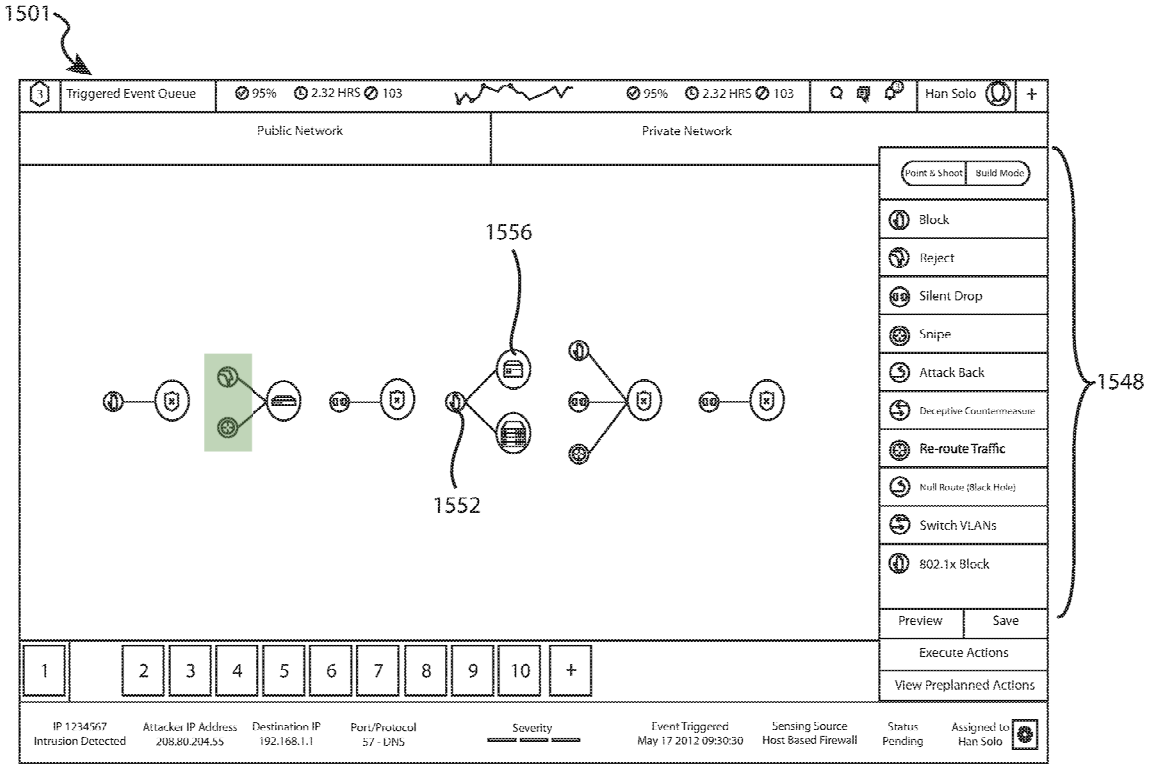


FIG. 15A

Thomas meets the parties' agreed construction of "in parallel," which is "concurrently or simultaneously." Ex. 1009 at 1. Thomas expressly states that the actions run "in parallel." Thomas also expressly contrasts that with running "in an order," thus showing that the parallel tasks occur concurrently or simultaneously. Ex. 1002, ¶ 155.

8. Claim 8

Claim 8, which depends from claim 1, further recites "wherein said collecting, by the SIEM device, results of the plurality of security tasks further comprises

normalizing the results." Ex. 1001, 18:60–62. This additional element of claim 8 would have been obvious over Thomas. Ex. 1002, ¶¶ 157–61.

Thomas explains that an "ingest processing component" may "normalize the probe data to a common analytical format." Ex. 1004, 13:5–10. Thomas also explains that its invention includes the system "normaliz[ing] to a single security event schema that can be acted upon at an abstract level." *Id.*, 1:54–67; Ex. 1002, ¶ 159.

Thomas meets Patent Owner's construction of "normalizing the results" as "transforming the results such that information from the results may be retained and saved in a unified format." Ex. 1009 at 22. Thomas expressly states the data is normalized. Additionally, consistent with Patent Owner's construction, Thomas teaches the normalization means transforming data to a unified format (e.g., the "common analytical format" or "single security event schema"). Ex. 1002, ¶ 160.

9. Claim 9

Claim 9, which depends from claim 1, further recites "performing asset correlation to the results of the plurality of security tasks; reporting the results of the plurality of security tasks if they are correlated to core network assets." Ex. 1001, 18:63–67. These additional elements of claim 9 would have been obvious over Thomas. Ex. 1002, ¶¶ 162–75.

a. [9a] "performing asset correlation to the results of the plurality of security tasks"

Thomas discloses this limitation. Ex. 1002, ¶¶ 164–70.

For example, Thomas discloses "an attribution functionality that matches data from various sources for the purpose of assigning the intent or identity to the action." Ex. 1004, 11:58–61. Thus, "the system maps many events to single actors, intents, and/or locations, or the reverse; one actor, intent, location profile to many events." *Id.*, 12:2–5; Ex. 1002, ¶ 165. Thomas further explains that the "cyber-data management node 104 may be viewed as a correlating engine for attack detection. Specifically, the cyber-data management node 104 uses a mediation component 108 to collect data from multiple probes and correlates the data to recognize an attack. The cyber-data management node 104 then uses an activation component 116 to coordinate the reactive steps required." Ex. 1004, 17:44–50. "Back-end aggregation, enrichment, and analysis of normal patterns of network behavior and ongoing analysis of current network behavior are provided to the ingest and mediation modules from network devices." *Id.*, 17:59–63; Ex. 1002, ¶ 166. Thomas shows its use of "Pattern Correlation" in Figure 6. Ex. 1002, ¶ 167.

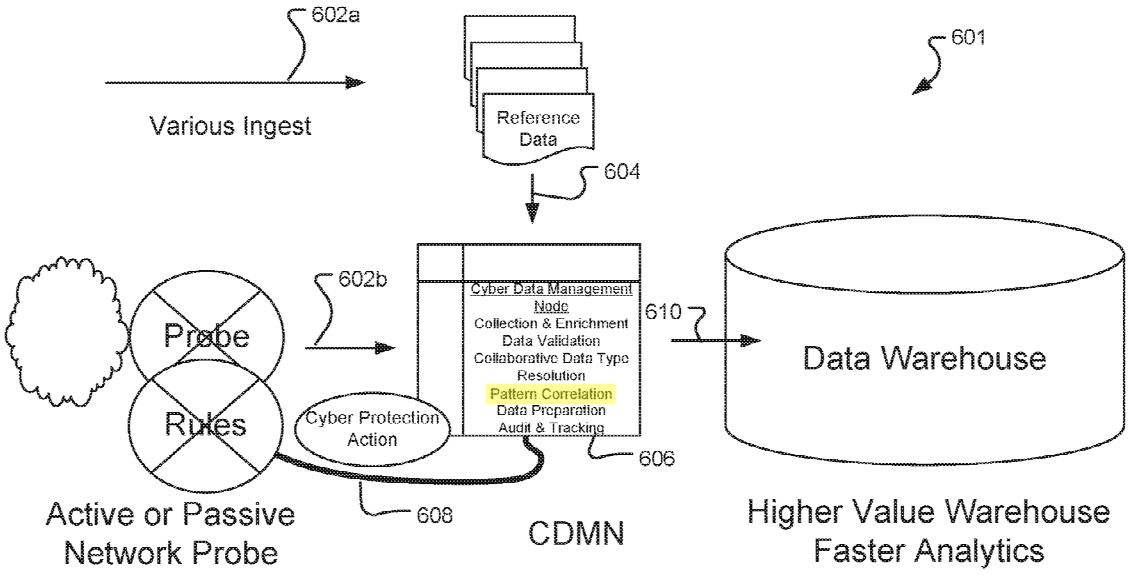


FIG. 6

600

Thus, a POSITA would understand that Thomas teaches asset correlation. Ex. 1002, ¶ 168. Thomas's description of performing "attribution" to one or more actors is an example of correlating a security threat to one or more network devices (assets). *Id.* For example, Thomas explains the system may "block external communication to and from infected machine(s), such as by reconfiguring the router 716, so that the infected machine are [sic] isolated." Ex. 1004, 21:12–16. A POSITA would understand this as an example of correlating data to identify assets (the infected machine(s)). Ex. 1002, ¶ 169.

b. [9b] "reporting the results of the plurality of security tasks if they are correlated to core network assets"

Thomas discloses this limitation. Ex. 1002, ¶¶ 171–75.

Thomas teaches that "[t]he activation component 116 can also provide pro-active responses to particular thresholds of events which can be pre-defined by a network administrator. The activation component 116 also provides alarms, e-mails, or other specific notifications to individuals, groups, or devices that require specific and immediate attention." Ex. 1004, 15:16–22. A POSITA would understand Thomas thus renders obvious reporting results if they are correlated to core network assets. Ex. 1002, ¶¶ 172–73. The administrator defines a threshold of event (e.g., by specifying that only events relating to core/important assets meet the threshold), and then Thomas reports based on that threshold. *Id.*. A POSITA would understand this would be a common way to implement Thomas's system: administrators frequently designate certain assets as more critical/core (e.g., because they contain sensitive data such as private user information, or because they are more costly hardware, or because of the resource's physical location), and they may focus additional resources on those assets, including additional reporting capability. *Id.*

Thomas meets Patent Owner's proposed construction of "core network assets" as "all or a subset of assets of the network designated by the administrator." Ex. 1009 at 21. As explained above, a POSITA would understand that Thomas's administrator-defined "threshold" is a way to define all or a subset of assets as "core" assets for which Thomas's system will report results as claimed. Ex. 1002, ¶ 174.

A POSITA would therefore understand that Thomas discloses each limitation of claim 9 and thus renders it obvious. Ex. 1002, ¶¶ 162–75.

10. Claim 10

Claim 10, which depends from claim 1, further recites "reporting the results of the plurality of security tasks based on an alert policy." Ex. 1001, 19:1–3. This additional element of claim 10 would have been obvious over Thomas. Ex. 1002, ¶¶ 176–80.

Thomas teaches that "[a]lerts, based on the configured rules, can be issued automatically." Ex. 1004, 19:7–10. Thomas also states the system may provide "automated alerts in an error and alarm logging (EAL) system." *Id.*, 19:11–17. Thomas further describes that the cyber-data management node may "alert[] other devices, firewalls and/or systems of an anomalous condition." *Id.*, 15:54–60. Thomas further states that it provides a "graphical user interface (GUI)" that may display, after performing an action, "which devices were successfully affected, or which failed in the attempt." *Id.*, 16:19–22. Thus, Thomas discloses providing reports (e.g., automated alerts, notifications on a GUI) based on an alert policy (e.g., the "configured rules"). Ex. 1002, ¶¶ 178–79.

11. Claim 15

Claim 15 would have been obvious under § 103(a) over Thomas. Ex. 1002, ¶¶ 181–94.

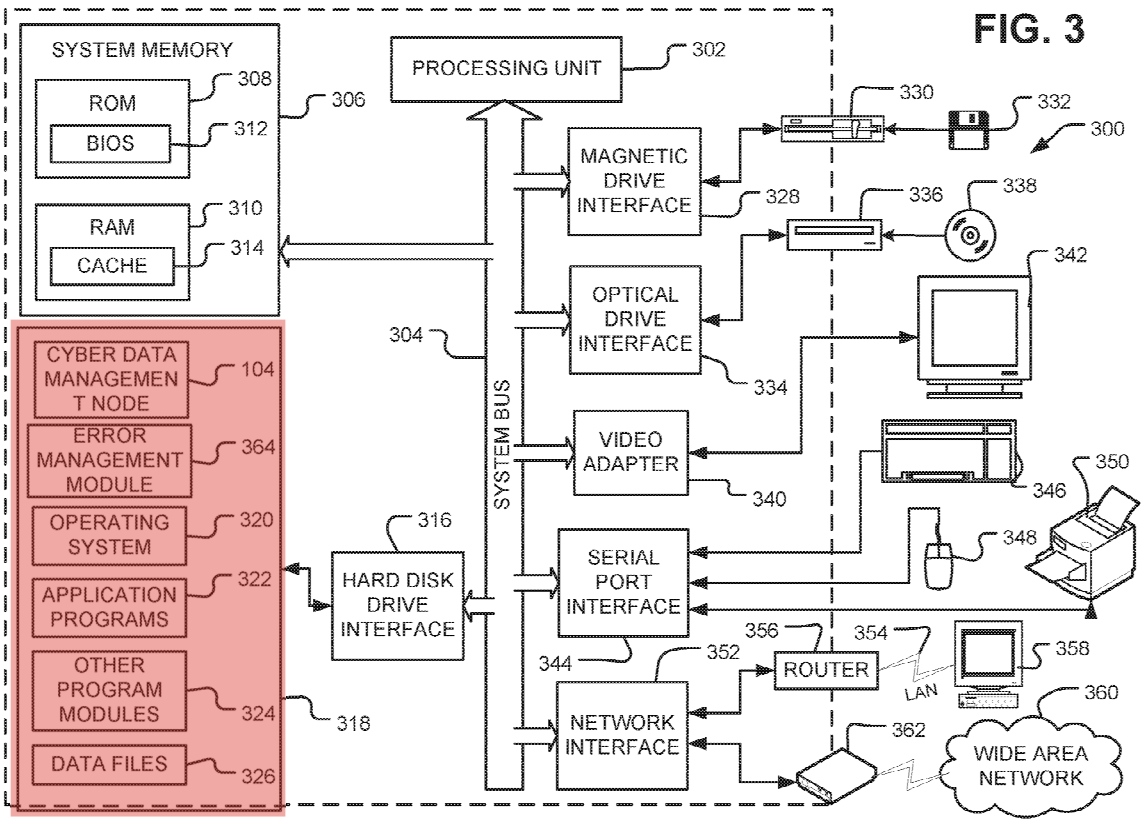
a. [15pre] "A security information and event management (SIEM) system comprising:"

As explained in connection with limitation [1a] ("creating, by a security information and event management (SIEM) device . . ."), Thomas discloses a SIEM. A POSITA would thus have found the subject matter of this limitation disclosed for the same reasons as limitation [1a], discussed above. *See* § VI.A.3.b; Ex. 1002, ¶¶ 182–83.

b. [15a] "non-transitory storage device having embodied therein instructions representing a security application; and"

Thomas discloses this limitation. Ex. 1002, ¶¶ 184–87.

Thomas depicts in Figure 3 an "exemplary computer system 300 for implementing the cyber-data management node 104." Ex. 1004, 8:57–59. As highlighted below in red, the system includes a "hard disk drive 318, for nonvolatile storage of applications, files, and data." *Id.*, 9:26–29; Ex. 1002, ¶ 185.



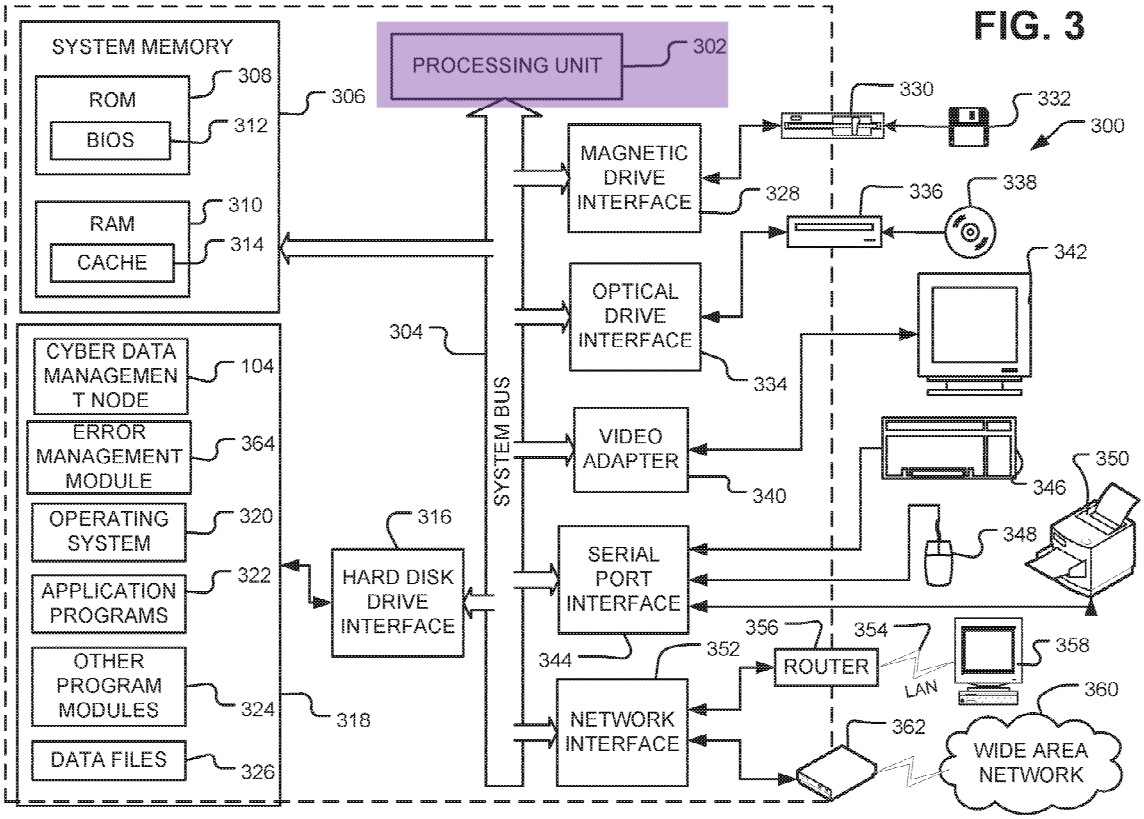
As explained in connection with the following limitations, this hard drive stores instructions representing an application (the cyber-data management node) that performs the recited claim steps. Ex. 1002, ¶ 186.

c. [15b] "one or more processors coupled to the non-transitory storage device and operable to execute the security application to perform a method comprising:"

Thomas discloses this limitation. Ex. 1002, ¶¶ 188–91.

Thomas explains that there "may be one or more processors 302, e.g., a single central processing unit (CPU), or a plurality of processing units, commonly referred to as a parallel processing environment (for example, a dual-core, quad-core, or other

multi-core processing device)." Ex. 1004, 9:10–14. An example processor is highlighted below in purple in Figure 3. Ex. 1002, ¶ 189.



As explained in connection with the following limitations, the processor executes the security application (the cyber-data management node) that performs the recited claim steps. Ex. 1002, ¶ 190.

d. [15b1] "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;"

e. [15b2] "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"

f. [15b3] "collecting results of the plurality of security tasks after they are performed by the one or more security devices."

The last three elements of claim 15 are substantively indistinguishable from the limitations [1a], [1b], and [1c]. Given that all remaining limitations in these elements are recited in claim 1, a POSITA would have found the subject matter of claim 9 obvious for the same reasons as claim 1, discussed above. *See* §§ VI.A.3.b, VI.A.3.c, and VI.A.3.d; Ex. 1002, ¶¶ 192–94.

12. Claim 18

Claim 18, which depends from claim 15, further recites "wherein the plurality of security tasks of the work flow are performed serially." Ex. 1001, 20:4–5. This additional element of claim 18 is substantively indistinguishable from the additional element required by claim 4. Given this, a POSITA would have found the subject matter of claim 18 obvious for the same reasons as claim 4, discussed above. *See* § VI.A.4; Ex. 1002, ¶¶ 195–96.

13. Claim 19

Claim 19, which depends from claim 18, further recites "wherein the method further comprises determining if a security task of the plurality of security tasks in the work flow should be performed based on the results of one or more previous security tasks of the plurality of security tasks of the work flow." Ex. 1001, 20:6–11. This additional element of claim 19 is substantively indistinguishable from the additional element required by claim 5. Given this, a POSITA would have found the subject matter of claim 19 obvious for the same reasons as claim 5, discussed above. *See* § VI.A.5; Ex. 1002, ¶¶ 197–98.

14. Claim 20

Claim 20, which depends from claim 18, further recites that "wherein the method further comprises transferring results of one or more previous security tasks of the plurality of security tasks of the work flow to a next security task of the plurality of security tasks of the work flow." Ex. 1001, 20:12–17. This additional element of claim 20 is substantively indistinguishable from the additional element required by claim 6. Given this, a POSITA would have found the subject matter of claim 20 obvious for the same reasons as claim 6, discussed above. *See* § VI.A.6; Ex. 1002, ¶¶ 199–200.

15. Claim 21

Claim 21, which depends from claim 15, further recites "wherein the plurality of security tasks of the work flow are performed in parallel." Ex. 1001, 20:18–19.

This additional element of claim 21 is substantively indistinguishable from the additional element required by claim 7. Given this, a POSITA would have found the subject matter of claim 21 obvious for the same reasons as claim 7, discussed above. *See* § VI.A.7; Ex. 1002, ¶¶ 201–02.

16. Claim 22

Claim 22, which depends from claim 15, further recites "wherein said collecting results of the plurality of security tasks further comprises normalizing the results." Ex. 1001, 20:20–22. This additional element of claim 22 is substantively indistinguishable from the additional element required by claim 8. Given this, a POSITA would have found the subject matter of claim 22 obvious for the same reasons as claim 8, discussed above. *See* § VI.A.8; Ex. 1002, ¶¶ 203–04.

17. Claim 23

Claim 23, which depends from claim 15, further recites "performing asset correlation to the results of the plurality of security tasks; reporting the results of the plurality of security tasks if they are correlated to core network assets." Ex. 1001, 20:23–29. These additional elements of claim 23 are substantively indistinguishable from the additional elements required by claim 9. Given this, a POSITA would have found the subject matter of claim 23 obvious for the same reasons as claim 9, discussed above. *See* § VI.A.9; Ex. 1002, ¶¶ 205–06.

18. Claim 24

Claim 24, which depends from claim 15, further recites "wherein the method further comprises reporting the results of the plurality of security tasks based on an alert policy." Ex. 1001, 20:30–32. This additional element of claim 24 is substantively indistinguishable from the additional element required by claim 10. Given this, a POSITA would have found the subject matter of claim 24 obvious for the same reasons as claim 10, discussed above. *See* § VI.A.10; Ex. 1002, ¶¶ 207–08.

B. Ground 2: Thomas in View of Gill Renders Claims 4–8 and 18–22 Obvious.

Claims 4–8 and 18–22 are invalid under 35 U.S.C. §103 over Thomas in view of Gill.

1. Summary of Gill

U.S. Patent App. Pub. No. 2012/0224057 to Gill et al. ("Gill") is titled "Situational Intelligence." Gill describes "blended risk assessment and security across logical systems, IT applications, databases, and physical systems from a single analytic dashboard, with auto-remediation capabilities." Ex. 1006, Abstract; Ex. 1002, ¶ 64.

Most relevant here, Gill describes various "workflows," which "define[] the number of stages during the completion of the tasks and various actor(s) involved at each stage. Each workflow has a set of conditions on which it is initiated." Ex. 1006,

¶ [0106]; Ex. 1002, ¶ 65. Gill states that the system "may be configured to automatically initiate a workflow action when potential security and compliance risk are detected." Ex. 1006, ¶ [0209]; Ex. 1002, ¶ 66. Gill also explains how to set up a workflow, including providing specific functions to initiate and schedule workflows, functions to specify input and output, and functions to convert information into standardized formats. Ex. 1006, ¶ [0574]; Ex. 1002, ¶ 67.

2. A POSITA Would Have Been Motivated to Combine Thomas and Gill.

Gill describes, in pertinent part, the use of "workflows" in a network security system. Ex. 1002, ¶ 210. As described above, Thomas teaches a network security system that uses workflows to perform various actions. *Id.*, ¶ 211. Thomas provides certain examples of actions that may be part of the workflow, but also states that the workflow may include "any appropriate automated action." Ex. 1004, 21:4–6. A POSITA would thus understand that Thomas's system could include any appropriate actions available in the prior art. Ex. 1002, ¶ 212. Gill's workflows provide further examples of workflows and appropriate actions that could be used in Thomas's system. *Id.*, ¶ 213. A POSITA would therefore be motivated to combine Gill's workflows into Thomas's system because it would be a simple, predictable application of known technology to provide additional appropriate actions for Thomas's system. *Id.* This combination would have achieved predictable results, i.e., making Gill's workflows and related commands available in Thomas's system.

Id., ¶ 214. The combination would have been fully operative in Thomas's invention and represents at most a simple substitution of Thomas's "any appropriate automated action" for the specific actions described in Gill. *Id.*

Furthermore, Gill and Thomas are references in the same field directed toward solving the same problems—i.e., using workflows and automated actions to improve network security and respond to threats in a networked computer system. Ex. 1002, ¶ 215; Ex. 1004, 1:50–54 ("The solution provides a dynamic adaptive defense (DAD) capable of receiving an indication of cyber threat and executing defined actions in an automated manner (with or without human intervention) to address that threat."), Ex. 1006, ¶ [0129] ("Ease of use of the workflow to support the compliance, controls, remediation and the approval process"). Given the similar problems being addressed, a POSITA would have looked to both references, including in combination, as a way to use automated workflows and tasks to improve network security. Ex. 1002, ¶ 216. Given that Thomas did not limit itself to any particular actions, a POSITA would have been motivated to combine the teachings of Thomas and Gill. *Id.* A POSITA would recognize that these similar references could readily be combined to provide a further improved solution that further enhances network security. *Id.*, ¶ 217.

Additionally, Thomas provides a specific motivation to combine. Thomas states that, as compared to the prior art, Thomas's invention is designed to provide

"improved command and control capability." Ex. 1002, ¶ 218; Ex. 1004, 7:65–8:5. Gill further improves the command and control capability by providing additional actions and ways to specify workflows. Ex. 1002, ¶ 218; Ex. 1006, ¶ [0574] (teaching specific functions for specifying and scheduling workflows). A POSITA would recognize that Gill's actions and workflows provide further ways to command and control the resources on the network, such that Thomas's system could rely on these additional actions and workflows to analyze and respond to threats to a private network. Ex. 1002, ¶ 219. Given that Thomas does not limit itself to any particular set of actions, a POSITA would be motivated to combine Thomas with Gill's teachings, which provide further actions and workflows that provides the improvement identified in Thomas. *Id.* A POSITA would recognize that this combination would meet the need identified in Thomas and would further improve network security, a goal shared by both Thomas and Gill. *Id.*, ¶ 220.

1. Claim 4

Claim 4, which depends from claim 1, further recites "wherein the plurality of security tasks of the work flow are performed serially." Ex. 1001, 18:47–48. As described above, Thomas alone renders claim 1 obvious. This additional element of claim 4 would have been obvious over Thomas in view of Gill. Ex. 1002, ¶¶ 222–29.

Gill describes "workflows," which "define[] the number of stages during the completion of the tasks and various actor(s) involved at each stage. Each workflow has a set of conditions on which it is initiated." Ex. 1006, ¶ [0106]. Gill states that the system "may be configured to automatically initiate a workflow action when potential security and compliance risk are detected." *Id.*, ¶ [0209]; Ex. 1002, ¶ 224. Gill explains how to set up a workflow, including specifying the scheduling and inputs/outputs. Ex. 1002, ¶ 225.

> 1.1 Workflow
> Workflow service can be found from spring application context using Service Locator and the below methods are defined.
> public boolean initiateWorkflow(long reqId, String userId);
> public boolean approveWorkflow(long reqId, String userId);
> public boolean rejectWorkflow(long reqId, String userId);
> public boolean holdWorkflow(long reqId, String userId);
> public List getAllTasksInProcess(long processId);
> . . .
> 1.2—Schedular
> Schedular can be found from spring application context using Service Locator and the below methods can be used to schedule the program.
> Specified program once

public boolean scheduleProgram (String programName);

Specified program once at specified date/time

public boolean scheduleProgram (String programName, Date startDate);

Specified program in a given interval at specified time/date:

public boolean scheduleProgram (String programName, Date startDate, Long duration);

Specified program in a given interval at specified start/end for time/date

public boolean scheduleProgram (String programName, Date startDate, Date endDate, Long duration);

1.4—Connector

Accepts Set of input params,

List of output params and retunrns [sic] single row map

Map invoke (Map inputParams, List outputParams) throws ALEApplicationException;

Accepts Set of input params,

List of output params and retunrns [sic] multiple row map

Map invoke2 (Map inputParams, List outputParams) throws ALEApplicationException;

Accepts Set of input params,

List of output params and retunrns [sic] void

Map invoke3 (Map inputParams, List outputParams) throws ALEApplicationException;

void close( ) throws ALEApplicationException;
void reconnect( ) throws ALEApplicationException;
void invoke3(Map inputParams, Map inoutTables) throws ALEApplicationException;

Ex. 1006, ¶ [0574].

A POSITA would understand that Gill discloses performing actions serially. Ex. 1002, ¶¶ 226–27. For example, the "holdWorkflow" function described above can allow one to hold a workflow action to be performed after another. Similarly, the "scheduleProgram" functions allow one to specify different workflows for different time periods, such that one workflow would be performed at a time period after the other, or serially.

Thomas in view of Gill meets the parties' agreed construction of "serially," which is "sequentially." Ex. 1009 at 1. The "scheduleProgram" allows the system to specify different workflows be performed sequentially in consecutive time periods, for example. Ex. 1002, ¶ 228.

2. Claim 5

Claim 5, which depends from claim 4, further recites "determining if a security task of the plurality of security tasks in the work flow should be performed based on the results of one or more previous security tasks of the plurality of security tasks of the work flow." Ex. 1001, 18:49–53. This additional element of claim 5 would have been obvious over Thomas in view of Gill. Ex. 1002, ¶¶ 230–34.

As described above, Gill describes various commands for specifying and scheduling the tasks in a workflow. Ex. 1006, ¶ [0574]. One of the commands Gill provides is "Map invoke," which allows the system to specify the inputs and outputs for a command. Using this, one could specify that the outputs of workflow action 1 should be the input to workflow action 2, or, in other words, that action 2 depends on the results of action 1. A POSITA would understand that using Gill's commands as such would allow one to determine whether to perform a task based on the results of previous tasks, which would be passed to the later task as an input. Ex. 1002, ¶¶ 232–33.

3. Claim 6

Claim 6, which depends from claim 4, further recites "transferring results of one or more previous security tasks of the plurality of security tasks of the work flow to a next security task of the plurality of security tasks of the work flow." Ex. 1001, 18:54–57. This additional element of claim 6 would have been obvious over Thomas in view of Gill. Ex. 1002, ¶¶ 235–39.

As described above, Gill describes various commands for specifying and scheduling the tasks in a workflow. Ex. 1006, ¶ [0574]. One of the commands Gill provides is "Map invoke," which allows the system to specify the inputs and outputs for a command. Using this, one could specify that the outputs of workflow action 1 should be the input to workflow action 2. Thus, Gill discloses transferring results

from one task to another. A POSITA would understand that using Gill's commands as such would allow one to pass results from one task to a later task as an input. Ex. 1002, ¶¶ 237–38.

4. Claim 7

Claim 7, which depends from claim 1, further recites "wherein the plurality of security tasks of the work flow are performed in parallel." Ex. 1001, 18:58–59. As described above, Thomas alone renders claim 1 obvious. This additional element of claim 7 would have been obvious over Thomas in view of Gill. Ex. 1002, ¶¶ 240–46.

As described above, Gill describes various commands for specifying and scheduling the tasks in a workflow. Ex. 1006, ¶ [0574]. For example, the "initiateWorkflow" function starts a workflow. Calling this function twice would result in two workflows being performed at the same time, in parallel. Additionally, the "scheduleProgram" functions allow one to specify different workflows for the same time period, such that one workflow would be performed at the same time period as the other, or in parallel. Ex. 1002, ¶¶ 242–44.

Thomas in view of Gill meets the parties' agreed construction of "in parallel," which is "concurrently or simultaneously." Ex. 1009 at 1. Gill's commands allow for two actions to be run in parallel by being initiated at the same time or by being scheduled for the same time period, i.e., concurrently. Ex. 1002, ¶ 245.

5. Claim 8

Claim 8, which depends from claim 1, further recites "wherein said collecting, by the SIEM device, results of the plurality of security tasks further comprises normalizing the results." Ex. 1001, 18:60–62. As described above, Thomas alone renders claim 1 obvious. This additional element of claim 8 would have been obvious over Thomas in view of Gill. Ex. 1002, ¶¶ 247–51.

Gill discloses various functions for converting information, such as a date or currency, to a standardized format:

> 1.9—Globalization
> Globalization has two parts to its component, Internalization and Localization.
> See slide [8] for information; starts with the login screen.
> Internalization -
> Displays labels and messages in specific languages based on user selection.
> GetI18NValue (key, local)
> → Returns labels for a given key in a given local format.
> Get118NValue (key)
> → Returns label for a given key in a default local format.
> Localization -
> Displays the dates and currencies in the local specific format.
> ConvertDatetoDBFormat (date)
> → Returns date in a default format.

ConvertDatetoDBFormat (date, pattern)

→ Returns date in a given pattern format.

ConvertDateToUIFormat (date)

→ Returns date in the specified date format.

The UI date format will be taken from the database.

ConvertCurrencyToDBFormat (currency)

→ Returns currency in a default format.

ConvertCurrencyToDBFormat (currency, format)

→ Returns currency in a given pattern format.

ConvertCurrencyToUIFormat (currency)

→ Returns currency in the specified date format.

The UI currency format will be taken from the database.

Ex. 1006, ¶ [0574]; Ex. 1002, ¶ 249.

Thomas in view of Gill meets Patent Owner's construction of "normalizing the results" as "transforming the results such that information from the results may be retained and saved in a unified format." Ex. 1009 at 22. The above functions in Gill transform results to a unified date or currency format. Ex. 1002, ¶ 250.

6. Claim 18

Claim 18, which depends from claim 15, further recites "wherein the plurality of security tasks of the work flow are performed serially." Ex. 1001, 20:4–5. This additional element of claim 18 is substantively indistinguishable from the additional element required by claim 4. Given this, a POSITA would have found the subject

matter of claim 18 obvious for the same reasons as claim 4, discussed above. *See* § VI.B.1; Ex. 1002, ¶¶ 252–53.

7. Claim 19

Claim 19, which depends from claim 18, further recites "wherein the method further comprises determining if a security task of the plurality of security tasks in the work flow should be performed based on the results of one or more previous security tasks of the plurality of security tasks of the work flow." Ex. 1001, 20:6–11. This additional element of claim 19 is substantively indistinguishable from the additional element required by claim 5. Given this, a POSITA would have found the subject matter of claim 19 obvious for the same reasons as claim 5, discussed above. *See* § VI.B.2; Ex. 1002, ¶¶ 254–55.

8. Claim 20

Claim 20, which depends from claim 18, further recites that "wherein the method further comprises transferring results of one or more previous security tasks of the plurality of security tasks of the work flow to a next security task of the plurality of security tasks of the work flow." Ex. 1001, 20:12–17. This additional element of claim 20 is substantively indistinguishable from the additional element required by claim 6. Given this, a POSITA would have found the subject matter of claim 20 obvious for the same reasons as claim 6, discussed above. *See* § VI.B.3; Ex. 1002, ¶¶ 256–57.

9. Claim 21

Claim 21, which depends from claim 15, further recites "wherein the plurality of security tasks of the work flow are performed in parallel." Ex. 1001, 20:18–19. This additional element of claim 21 is substantively indistinguishable from the additional element required by claim 7. Given this, a POSITA would have found the subject matter of claim 21 obvious for the same reasons as claim 7, discussed above. *See* § VI.B.4; Ex. 1002, ¶¶ 258–59.

10. Claim 22

Claim 22, which depends from claim 15, further recites "wherein said collecting results of the plurality of security tasks further comprises normalizing the results." Ex. 1001, 20:20–22. This additional element of claim 22 is substantively indistinguishable from the additional element required by claim 8. Given this, a POSITA would have found the subject matter of claim 22 obvious for the same reasons as claim 8, discussed above. *See* § VI.B.5; Ex. 1002, ¶¶ 260–61.

C. Secondary Considerations

As far as Forescout is aware, Fortinet has never alleged any secondary considerations that would be relevant to an obviousness determination of any claims of the '421 patent. Should Fortinet allege any secondary considerations in the future, Forescout reserves its rights to respond to those allegations.

VII. Mandatory Notices

A. Real Parties-in-Interest

The real party-in-interest in this proceeding is Forescout Technologies, Inc., who is the sole party who has funded this petition and who has full and exclusive control over these proceedings.

B. Related Proceedings

Fortinet has asserted the '421 patent against Forescout in the Northern District of California, Case No. 3:20-cv-03343-EMC. There appear to be no pending applications that claim priority to the '421 patent.

This identification of related matters is based on information currently known to Petitioner based on a reasonably diligent search of publicly available materials. Patent Owner may be aware of additional proceedings—including proceedings before the Board or otherwise before the Office—relating to patent claims encompassing similar subject matter or raising similar issues to those involved here.

C. Lead and Backup Counsel

Forescout's lead and backup counsel are:

Lead Counsel for Petition	Backup Counsel for Petition
Katherine A. Vidal (Reg. No. 46,333) Winston & Strawn LLP 275 Middlefield Rd, Suite 205 Menlo Park, California 94025 kvidal@winston.com T: 650.858.6500, F: 650.858.6550	Louis L. Campbell (Reg. No. 59,963) Matthew R. McCullough (*pro hac vice* to be filed) James C. Lin (*pro hac vice* to be filed) Winston & Strawn LLP 275 Middlefield Rd, Suite 205 Menlo Park, California 94025

Lead Counsel for Petition	Backup Counsel for Petition
	llcampbell@winston.com mrmccullough@winston.com jalin@winston.com T: 650.858.6500, F: 650.858.6550 Kimball R. Anderson (*pro hac vice* to be filed) Winston & Strawn LLP 35 W. Wacker Drive Chicago, Illinois 60601 kanderso@winston.com T: 312.558.5600, F: 312.558.5700

D. Electronic Service

Forescout consents to electronic service at: Winston-Forescout-Fortinet-IPRs@winston.com.

VIII. Institution of This *Inter Partes* Review Is Proper Under 35 U.S.C. §§ 314(a) and 325(d).

A. The *Fintiv* Factors Favor Institution

The factors set forth in *Apple, Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Precedential) favor institution.

1. Potential for Stay: There is a strong likelihood for a stay of the litigation. The presiding judge, the Honorable Edward M. Chen, has granted motions to stay pending IPR where the IPR was instituted at an early stage of the litigation. Ex. 1010 at 3–9; Ex. 1011 at 6–13. In the litigation, no trial date has been set and claim construction has not yet occurred. Forescout intends to move to stay the litigation

pending IPR.

Moreover, as described in detail below for factors 3–4, this IPR raises prior art not previously considered during prosecution. The strong likelihood for a stay, and the low risk of duplicative efforts, weigh in favor of institution.

2. Proximity of the Court's Trial Date: A trial date for the parties' litigation has not yet been set. It is therefore likely that this IPR would be completed prior to trial. Factor 2 therefore favors institution.

3&4. Investment in Parallel Proceeding & Overlap of Issues: Given the early stages of the litigation, the risk of duplicating work already completed by the court and/or the respective parties is mitigated. Notably, the invalidity issues raised in this IPR do not overlap with issues raised in prosecution. No validity-related issues have been raised to the court in the pending litigation, and the court has not set deadlines for expert discovery. Factors 3 and 4 therefore favor institution.

5. Whether Same Party: The same parties are at issue in both the litigation and here. However, in light of the early stage and minimal overlap in issues, this factor should not weigh against institution.

6. Other Factors Including the Merits: Because the merits of this IPR are exceedingly strong, factor 6 favors institution.

B. Institution Is Proper Under 35 U.S.C. § 325(d)

"[U]nder § 325(d), the Board uses the following two-part framework:

(1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of [the] first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims." *Advanced Bionics, LLC v. Med-El Electromedizinische Gerate GMBH*, IPR2019-01469, Paper 6. Here, neither condition of the first part of the framework is met.

The Thomas and Gill references relied upon in this petition were not considered during examination of the '421 patent. *See generally* Ex. 1007 at 69–76, 91–103, 109–16. Moreover, Thomas and Gill are not cumulative of any previously considered art and do not rely on arguments overlapping with those considered during examination or reexamination.

C. The *General Plastic* Factors Do Not Apply

Forescout has never previously filed a petition for *inter partes* review of the '421 patent. This is Forescout's first petition on this patent; it is not a "follow-on petition." But even if it were, "[t]here is no *per se* rule precluding . . . follow-on petitions," although the Board will consider the equities in determining whether to institute review. *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, No. IPR2016-01357, 2017 WL 3917706, at *7 (P.T.A.B. Sept. 6, 2017) (precedential decision). *General Plastic* set forth a list of factors to consider in

determining whether to institute a follow-on petition. *Id.* at *7–8. Even if this were a "follow-on" petition, the *General Plastic* factors show that institution of this petition would be equitable and not unduly prejudicial to Fortinet.

- The first five factors favor institution because this is Forescout's first petition on this patent.
- Factor 6 favors institution because the Board has not previously spent resources considering the issues in this petition.
- Factor 7 is neutral because this petition would not seem to affect the Board's ability to timely issue a final determination.

For these reasons, the Board should not exercise its discretion to deny institution of this petition.

IX. Fees

The required fee is being paid electronically through PTAB E2E.

X. Conclusion

For at least the foregoing reasons, claims 1, 4–10, 15, and 18–24 of the '421 patent would have been obvious to a POSITA under 35 U.S.C. § 103. Petitioner therefore requests *inter partes* review of the '421 patent and cancellation of the challenged claims.

Dated: August 11, 2021 Respectfully submitted,

/ Katherine A. Vidal /
Katherine A. Vidal (Reg. No. 46,333)
Louis L. Campbell (Reg. No. 59,963)
Matthew R. McCullough (*pro hac vice* to be filed)
James C. Lin (*pro hac vice* to be filed)
WINSTON & STRAWN LLP
275 Middlefield Rd, Suite 205
Menlo Park, California 94025
kvidal@winston.com
llcampbell@winston.com
mrmccullough@winston.com
jalin@winston.com
T: 650.858.6500, F: 650.858.6550

Kimball R. Anderson (*pro hac vice* to be filed)
WINSTON & STRAWN LLP
35 W. Wacker Drive
Chicago, Illinois 60601
kanderso@winston.com
T: 312.558.5600, F: 312.558.5700

Counsel for Petitioner Forescout Technologies, Inc.

CERTIFICATE OF COMPLIANCE

This petition complies with the word count limits set forth in 37 C.F.R. § 42.24(a)(1)(i) because this petition contains 11,562 words, excluding the parts of the petition exempted by 37 C.F.R. § 42.24(a)(1) and determined using the word count provided by Microsoft Word, which was used to prepare this petition.

Dated: August 11, 2021

Respectfully submitted,

/ *Katherine A. Vidal* /

Katherine A. Vidal (Reg. No. 46,333)
WINSTON & STRAWN LLP
275 Middlefield Rd, Suite 205
Menlo Park, California 94025
kvidal@winston.com
T: (650)858-6500; F: (650)858-6550

Counsel for Petitioner Forescout Technologies, Inc.

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), this is to certify that on August 11, 2021, I caused to be served a true and correct copy of the foregoing "**PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1, 4–10, 15, AND 18–24 OF U.S. PATENT NO. 9,503,421**" and Exhibits 1001 – 1011 by FedEx on the Patent Owner at the correspondence address of record for U.S. Patent No. 9,503,421:

MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

A courtesy copy of this petition and supporting material was also served upon litigation counsel for Patent Owner via email, as follows:

John M. Neukom
Skadden Arps Slate Meagher & Flom LLP
525 University Avenue, Suite 1400
Palo Alto, CA 94301-1908
Email: John.Neukom@skadden.com

/ Katherine A. Vidal /

Katherine A. Vidal (Reg. No. 46,333)
WINSTON & STRAWN LLP
275 Middlefield Rd, Suite 205
Menlo Park, California 94025
kvidal@winston.com
T: (650)858-6500; F: (650)858-6550

Counsel for Petitioner Forescout Technologies, Inc.