

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

QOMPLX LLC,
Patent Owner.

Case IPR2026-00325
Patent 12,301,627

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. PETITIONER’S GROUNDS FAIL (ALL CLAIMS, ALL GROUNDS).....	4
A. Petitioner Fails To Show That Stokes Teaches A “Relationship Between A Respective Pair Of Entities” (All Claims, All Grounds).....	4
1. The ’627 Patent Confirms That “Relationship[s]” And “Event[s]” Are Distinct.....	5
2. Petitioner Fails To Prove That Stokes’s Events Are The Claimed Relationships.	12
a. Petitioner And Dr. Black Provide No Reasoned Basis To Conclude That Stokes’s Events Are Relationships.	14
b. Stokes’s Individual Event Records Do Not Establish The Claimed Relationships.....	17
c. Stokes’s Generic Graph Statement Does Not Change The Fact That Stokes’s “Edges Represent Events.”	21
B. Petitioner Fails To Demonstrate That Stokes-Crabtree Discloses Or Renders Obvious The Claimed Attack Path Limitations (All Claims, All Grounds).	23
1. The Claims Require Identifying Attack Paths From The Newly Added Entity Before The Claimed Path Has Already Been Traversed.	24
a. The Claimed Attack Path Analysis Must Be Based On The Modified Graph And Must Involve The Newly Added Entity.....	25

b.	The Claimed Attack Path Analysis Identifies Potential Exposure, Not Nodes Already Compromised By Prior Traversal.	26
2.	Petitioner’s Stokes-Crabtree Theory Does Not Satisfy Either Claim Requirement.	31
3.	Petitioner Cannot Fill The Gap With Unsupported “Obvious Use Case” Testimony.	38
III.	CONCLUSION	47

TABLE OF AUTHORITIES

Page(s)

COURT DECISIONS

<i>ACCO Brands, Inc. v. Micro Sec. Devices, Inc.</i> , 346 F.3d 1075 (Fed. Cir. 2003)	30
<i>Arendi S.A.R.L. v. Apple, Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	45
<i>Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.</i> , 533 F.3d 1362 (Fed. Cir. 2008)	6
<i>Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP</i> , 616 F.3d 1249 (Fed. Cir. 2010)	6, 7
<i>Bettcher Indus., Inc. v. Bunzl USA, Inc.</i> , 661 F.3d 629 (Fed. Cir. 2011)	42
<i>D’Agostino v. MasterCard Int’l Inc.</i> , 844 F.3d 945 (Fed. Cir. 2016)	30
<i>DSS Tech. Mgm’t v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	45
<i>Ekchian v. Home Depot, Inc.</i> , 104 F.3d 1299 (Fed. Cir. 1997)	29
<i>Engel Indus. v. Lockformer Co.</i> , 96 F.3d 1398 (Fed. Cir. 1996)	7, 15
<i>Gaus v. Conair Corp.</i> , 363 F.3d 1284 (Fed. Cir. 2004)	6
<i>In re Conrad</i> , 759 Fed. App’x. 982 (Fed. Cir. 2019)	47

<i>In re Facebook, Inc.</i> , 743 F. App'x 998 (Fed. Cir. 2018) (nonprecedential)	42
<i>In re Felton</i> , 484 F.2d 495 (C.C.P.A. 1973)	42
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	43
<i>InTouch Techs., Inc. v. VGo Commc'ns., Inc.</i> , 751 F.3d 1327 (Fed. Cir. 2014)	46
<i>K/S HIMPP v. Hear-Wear Techs., LLC</i> , 751 F.3d 1362 (Fed. Cir. 2014)	45
<i>Magnolia Med. Techs., Inc. v. Kurin, Inc.</i> , 169 F.4th 1094 (Fed. Cir. 2026)	7
<i>Otsuka Pharm. Co., v. Sandoz, Inc.</i> , 678 F.3d 1280 (Fed. Cir. 2012)	46
<i>Saffran v. Johnson & Johnson</i> , 712 F.3d 549 (Fed. Cir. 2013)	29
<i>Spectrum Int'l, Inc. v. Sterilite Corp.</i> , 164 F.3d 1372 (Fed. Cir. 1998)	29
<i>Univ. of Strathclyde v. Clear-Vu Lighting LLC</i> , 17 F.4th 155 (Fed. Cir. 2021)	46
<i>Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	16, 44

AGENCY DECISIONS

Cisco Sys., Inc. v. C-Cation Techs., LLC,
IPR2014-00454, Paper 12 (Aug. 29, 2014)
(informative)40

Xerox Corp. v. Bytemark, Inc.,
IPR2022-00624, Paper 9 (Aug. 24, 2022)
(precedential) 16, 44

REGULATIONS

37 C.F.R. § 42.6(a)(3)40

37 C.F.R. § 42.65(a)..... 16, 44

EXHIBIT LIST	
2001	Declaration of Nathan Lowenstein in Support of Notice of Intent
2002	Declaration of Colette Woo in Support of Notice of Intent
2003	Declaration of Sam Malek, Ph.D. [Malek Decl.]
2004	Relationship, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/relationship (accessed July 8, 2026) [Merriam Webster – Relationship]
2005	Event, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/event (accessed June 10, 2026) [Merriam Webster – Event]

All emphases are added unless otherwise stated.

I. INTRODUCTION

The Petition should be denied because Petitioner fails to demonstrate a reasonable likelihood of prevailing as to any challenged claim. Petitioner's grounds fail for two independent reasons.

First, Petitioner fails to demonstrate that Stokes teaches the claimed "relationship[s]" between entity pairs. The claims require that the stored graph include edges, "wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities." Ex. 1001 ['627] cls. 1, 18. Petitioner's mapping depends on equating Stokes's disclosed events with the claimed relationships. But Petitioner never justifies that equivalence.

"Events" and "relationships" are different claim terms and play different roles: event data is received, while relationships are identified and represented by graph edges. *See* Section II.A.1. Ignoring that distinction in the intrinsic record, Petitioner relies on Stokes's disclosure that graph edges model "computer-to-computer connections or user logon *events*." Pet., 21-22. Indeed, Petitioner and its expert, Dr. Black, concede that "*edges in Stokes represent events*." Pet., 37-38; Ex. 1003 [Black Decl.] ¶ 122. But Petitioner never explains why Stokes's events constitute a relationship. Moreover, Petitioner's own later mapping only confirms the disconnect: when addressing limitations that recite "events," Petitioner treats the same edges in Stokes as events rather than relationships. *See* Pet., 37-39

(“edges in Stokes represent events”). Petitioner provides no explanation for how Stokes’s events can qualify as both the claimed “events” and the claimed “relationships.” *See* Section II.A.2.

Second, Petitioner independently fails to demonstrate that the Stokes-Crabtree combination discloses or renders obvious the claimed attack path limitations. The independent claims require using the modified graph to analyze attack paths involving a new entity added by the graph modification. In claim 1, the attack path must be identified based on the modified graph and must involve a newly added first entity. Ex. 1001 [’627] cl. 1. In claim 18, the graph is modified to add a newly identified third entity, and the later-identified attack paths must include an attack path comprising that third entity. *Id.*, cl. 18. During prosecution, the Applicant made clear that the attack path is forward looking, further making clear that the Neil prior art reference did not satisfy the claims because it identified “*where the attacker has already been in the network,*” and that the Altman reference was “based on message traversal through the network *that has already happened.*” Ex. 1002 [Pros. Hist.] 237-238. The Applicant made clear that this distinction applied to claim 18 as well. *Id.*, 238. The Examiner agreed and allowed the claims, and further amended claim 1 to require an attack path that “could be involved” in an attack and entities that “can be reached” through the modified graph, confirming the distinction the Applicant drew during prosecution.

Id., 276, 278-280; *see* Section II.B.1.

Stokes’s approach does not involve a new entity added to an updated graph and ask what attack paths could use that entity. It begins with a node already known to be malicious or compromised; it is not an analysis directed towards or involving the newly added node. From that compromised node, Stokes follows inbound and outbound paths to identify—like Neil and Altman—other *already* compromised computers or accounts along the attacker’s lateral-movement path. Pet., 30-32; Ex. 1004 [Stokes] [0028], [0066]. That is the same backwards-looking analysis of “where the attacker has already been in the network” and of a traversal “that has already happened” that the Applicant distinguished and disclaimed in prosecution. *See* Section II.B.2.

Crabtree does not make up for Stokes’s shortcomings. Petitioner uses Crabtree for graph updating, but still uses Stokes for the path analysis. A newly updated graph does not change Stokes’s starting point or purpose: Stokes still starts from a compromised node and looks for other already compromised nodes. Petitioner asserts that the combined system “would apply” Stokes’s path analysis to paths involving newly added nodes (Pet., 32), but neither the Petition nor Dr. Black identifies evidence or reasoning that would turn Stokes’s backward-looking compromised-node investigation into the claimed analysis of potential attack paths involving the entity newly added by the graph modification. *See* Section II.B.3.

Ground 2 does not cure these defects. That ground adds Sekar only for claim 3, and does not rely on Sekar to supply the missing relationship or attack path limitations in the independent claims. Accordingly, Ground 2 fails for the same reasons as Ground 1.

Because Petitioner fails to demonstrate a reasonable likelihood of prevailing, the Director should deny institution.

II. PETITIONER’S GROUNDS FAIL (ALL CLAIMS, ALL GROUNDS).

A. Petitioner Fails To Show That Stokes Teaches A “Relationship Between A Respective Pair Of Entities” (All Claims, All Grounds).

The claims require that the stored representation of the first graph must include edges, “wherein each edge of the first plurality of edges corresponds *to a respective relationship between a respective pair of entities.*” Ex. 1001 [’627] cls. 1, 18. Petitioner therefore must show that Stokes teaches “relationships” between entity pairs—not merely events involving entity pairs.

Petitioner does not make that showing. Its theory depends on treating Stokes’s event edges as the claimed relationships. For the existing graph edges, Petitioner relies on Stokes’s disclosure that graph edges model “computer-to-computer connections or user logon *events*,” and on Stokes’s generic notation describing “connection relationships ... between pairs of nodes.” Pet., 21-22. This

is undisputed: both Petitioner and its expert freely admit that “edges in Stokes represent events.” Pet., 37-38; Ex. 1003 [Black-Decl.] ¶ 122 (same).

Petitioner does not—and cannot—justify the equivalence it draws between events and relationships. The claim language and specification separately recite events and relationships and assign them different roles: event data is received, while relationships are identified and represented by graph edges. *See* Section II.A.1. Petitioner ignores that distinction and fails to demonstrate that Stokes’s event and connection disclosures satisfy the claimed “relationships” between entities. *See* Section II.A.2.

1. The ’627 Patent Confirms That “Relationship[s]” And “Event[s]” Are Distinct.

Contrary to the premise of Petitioner’s argument, the claim language and specification confirm that events and relationships are distinct. Starting with the claim language itself, “events” and “relationship[s]” are different claim terms. For instance, claim 1 requires:

receive streaming data comprising time-stamped data about *events*
relating to one or more entities of the first plurality of entities,

and then requires:

based on a second portion of the streaming data ... identify a first
relationship between a pair of entities

Ex. 1001 [’627] cl. 1; *see also id.*, cl. 18 (similarly reciting “streaming data comprising time-stamped data about events,” then “identify a first relationship between a pair of entities”).

The claims also distinguish the roles that “events” and “relationships” perform. The system receives data “about events” and, based on that data, identifies a “relationship” between entities. The claims do not describe receiving event data and merely identifying the event described by that data. Rather, the event data is the input from which the relationship is identified. If “event” and “relationship” meant the same thing, the claim could simply require identifying an event from the received event data. Instead, the claim requires identifying a relationship based on data about events, confirming that the two concepts are different. Ex. 2003 [Malek Decl.] ¶ 37.

Basic claim-construction principles reinforce the same point. “Event” and “relationship” are different claim terms, and “[d]ifferent claim terms are presumed to have different meanings.” *Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1371 (Fed. Cir. 2008). And where, as here, “a claim lists elements separately, ‘the clear implication of the claim language’ is that those elements are ‘distinct component[s]’ of the patented invention.” *Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (quoting *Gaus v. Conair Corp.*, 363 F.3d 1284, 1288 (Fed. Cir. 2004); *see also Engel Indus.*

v. Lockformer Co., 96 F.3d 1398, 1405 (Fed. Cir. 1996) (concluding that separately recited “second portion” and “return portion” “logically cannot be one and the same”); *Magnolia Med. Techs., Inc. v. Kurin, Inc.*, 169 F.4th 1094, 1102 (Fed. Cir. 2026) (“*Becton* thus stands for the proposition that when claim limitations are separately listed within a claim, that implies that the claim’s *plain and ordinary meaning* requires separate corresponding structures.”) (emphasis in original).

In accord, the ’627 patent’s specification likewise treats relationships as distinct from events. It describes graph edges as relationships between entities, not merely as records that an event occurred. As Dr. Malek explains:

The ’627 patent explains that a “graph” is a “representation of information and relationships,” where each primary unit of information is a “node” or “vertex,” and “the relationship between two nodes makes up an edge of the graph.” Ex. 1001 [’627] 7:45-49. The specification further explains that a relationship forming an edge may be qualified by a “label”; for example, an edge indicating that two people know each other may be labeled “knows.” *Id.*, 7:49-58. Thus, the patent describes graph edges as relationships between nodes, not merely as records that an event occurred.

The specification then applies that same understanding to a cybersecurity graph. It explains that “[a] cyber-physical graph 1902 represents the relationships between entities associated with an organization ...” Ex. 1001 [’627] 28:6-8. The ’627 specification

illustrates several examples of these relationships in, for instance, Figure 22:

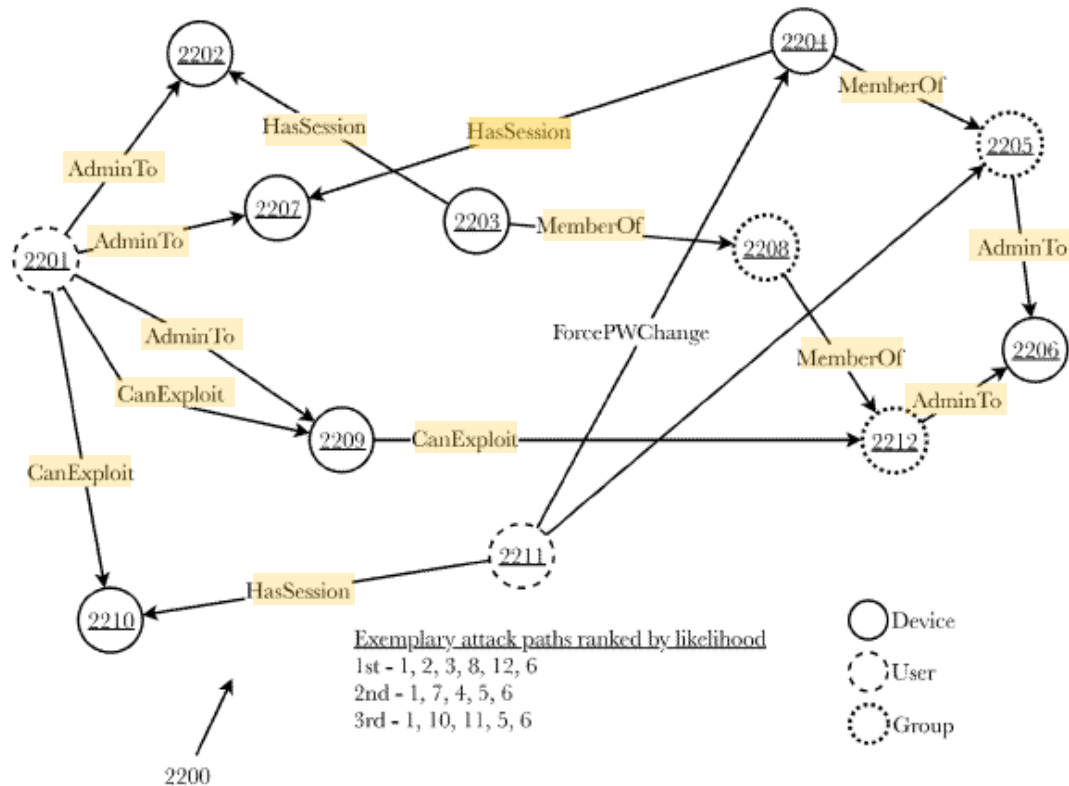


Fig. 22

Id., Fig. 22 (annotated); 28:40-43 (“The edges (lines) between the nodes indicate relationships between the nodes, and have a direction and relationship indicator such as ‘AdminTo,’ ‘MemberOf,’ etc.”). As can be seen above, the indicators describe the current relationship between the entities in the network. For instance, we can see that device 2204 is a member of group 2205 which administers device 2206.

The specification also describes the resulting graph visualization as one that correlates physical relationships, such as a user’s personal

computer or physical connections between servers, with logical relationships, such as access privileges or database connections, “to produce a meaningful and contextualized visualization of a security infrastructure that reflects the current state of the internal relationships present in the infrastructure.” Ex. 1001 [’627] 24:6-14. Similarly, the specification explains that the system can “maintain an up-to-date model of the network in real-time.” *Id.*, 26:5-6. These disclosures illustrate the specification’s usage: the graph models relationships among entities, while event data supplies information that may update that model.

Ex. 2003 [Malek Decl.] ¶¶ 39-41.

Events, by contrast, are described as something that happens or an occurrence. As Dr. Malek explains:

The specification’s example of an event—“an attempted attack against a vulnerable system or resource”—describes something that happens. Ex. 1001 [’627] 24:61-62. Standing alone, an attempted attack may provide information relevant to a relationship, but it does not itself identify the relationship between the involved entities, much less the type of relationship represented by the ’627 patent’s graph edges. The specification therefore treats events as information that may be logged, analyzed, and used to update relationship information; it does not treat “event” and “relationship” as interchangeable terms.

Ex. 2003 [Malek Decl.] ¶ 42.

Figure 11 is further instructive, and it too distinguishes event data from relationships.

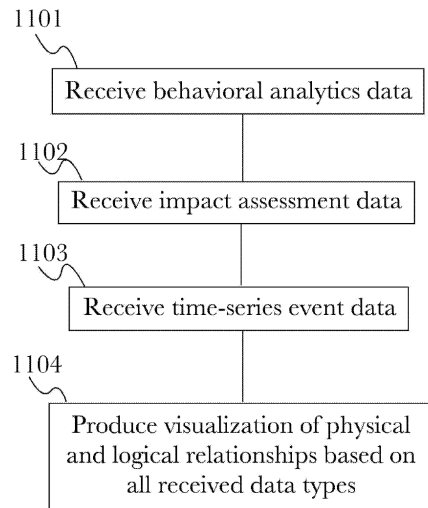


Fig. 11

1100

Ex. 1001 [’627] Fig. 11. Figure 11 concerns receiving various types of information, including time-series event data 1103, and using that information:

to produce 1104 a graph visualization of users, servers devices, and other resources correlating physical relationships (such as a user’s personal computer or smartphone, or physical connections between servers) with logical relationships (such as access privileges or database connections), to produce a meaningful and contextualized visualization of a security infrastructure that reflects the current state of the internal relationships present in the infrastructure.

Id., 24:6-14. The immediately preceding sentence explains that the time-series information is “received and incorporated, updating CPG information as changes

occur and events are logged.” *Id.*, 24:2-5. Thus, Figure 11 mirrors the claim structure: event data is received and incorporated, while the resulting graph visualization represents physical and logical relationships. Event data may be an input from which relationship information is derived or updated, but the patent does not treat the event data and the identified relationship as the same thing.

The ordinary meanings of “event” and “relationship” confirm the distinction reflected in the claim language and specification. As Dr. Malek explains:

A “relationship” is “the way in which two or more things ... are connected” or “the state of being related or interrelated.” Ex. 2004 [Merriam Webster – Relationship]. By contrast, an “event” is “something that happens” or an “occurrence.” Ex. 2005 [Merriam Webster – Event]. Thus, the ordinary meanings of these terms align with the ’627 patent’s treatment of relationships and events. The patent’s relationship indicators (such as “AdminTo,” “MemberOf,” and “HasSession”) describe how entities are connected to one another. Ex. 1001 [’627] 28:42-43, Fig. 22.

Ex. 2003 [Malek Decl.] ¶ 45.

Accordingly, the claim language, specification, and ordinary meanings all confirm that “event” and “relationship” are not interchangeable. The claims themselves contemplate using event data to identify relationships, but that reinforces the distinction; it does not permit Petitioner to satisfy the relationship limitations merely by identifying an event involving two entities and declaring they

are a relationship. Petitioner still had to identify the relationship allegedly taught by Stokes and explain why Stokes's event record satisfies the relationship limitations. As explained below, neither the Petitioner nor Dr. Black makes this showing.

2. Petitioner Fails To Prove That Stokes's Events Are The Claimed Relationships.

Petitioner's analysis of the limitation-at-issue rests upon an unsupported equivalence: that a Stokes event is the claimed relationship. Petitioner relies on Stokes's disclosure that graph edges model "computer-to-computer connections or user logon *events*" and on Stokes's general mathematical notation referring to "connection relationships":

Stokes discloses that its graph "edges" model "computer-to-computer connections or user logon *events*." EX1004, [0025]. Stokes also teaches using the known mathematical representation of a graph, with "E" representing "the set of connection relationships ... between pairs of nodes, called edges." EX1004, [0026]; *supra* Section VII.A. Thus, in the Stokes graph, each of the plurality of edges corresponds to a relationship between a respective pair of nodes. EX1003, ¶81.

Pet., 21-22. Dispositively, Petitioner and Dr. Black concede that "edges in Stokes represent events." *Id.*, 37-38 ("edges in Stokes represent events"); Ex. 1003 [Black Decl.] ¶ 122 (same).

Petitioner, thus, does not satisfy the limitation-in-question which requires

that “each edge of the first plurality of edges corresponds to a respective *relationship* between a respective pair of entities of the first plurality of entities.”

Ex. 1001 [’627] cls. 1, 18. Thus, Petitioner had to establish that Stokes’s mapped edges correspond to *relationships*—not *events*—between entity pairs.

Petitioner’s failure is not merely a matter of terminology. As explained below, the evidentiary record exposes the missing relationship in three related respects. First, neither the Petition nor Dr. Black provides technical reasoning supporting the asserted equivalence between Stokes’s events and the claimed relationships; Dr. Black substantially repeats the Petition’s conclusion without adding independent technical analysis. *See* Section II.A.2(a). Second, Stokes’s actual disclosures characterize its individual edges as records of particular, time-stamped events, not the claimed relationships. *See* Section II.A.2(b). Finally, Stokes’s generic statement concerning graph edges does not change the fact that the edges Petitioner relies upon—by its own admission—reflect events, not relationships. *See* Section II.A.2(c); Pet., 37-38; Ex. 1003 [Black Decl.] ¶ 122. These deficiencies confirm that Petitioner has identified events between nodes, but not the relationships between pairs of entities required by the claims.

a. *Petitioner And Dr. Black Provide No Reasoned Basis To Conclude That Stokes's Events Are Relationships.*

Petitioner's theory depends on an unstated and unsupported premise.

Although the claims separately recite data "about events" and identified "relationship[s]," Petitioner argues that Stokes's "computer-to-computer connection and user logon events" are the claimed relationships. Petitioner thus treats "events" and "relationships" as interchangeable for purposes of its Stokes mapping. Petitioner provides no basis for that equivalence in the claim language, the specification, the prosecution history, or the extrinsic record.

And, as explained above, Petitioner's premise is wrong. The claims and specification distinguish data "about events" from the relationships identified based on that data and represented in the graph. *See* Section II.A.1. Petitioner, however, never acknowledges or addresses that distinction. *See* Pet., 21-22. Petitioner never identifies the relationship allegedly taught by a Stokes event, or explains why the event occurrence itself constitutes that relationship. Instead, Petitioner simply substitutes "relationship" for Stokes's "event" and proceeds, without explanation, as though the limitation has been met.

Indeed, Petitioner continues to shift between "relationship" and "event" elsewhere in the Petition without acknowledging the distinction. For the "relationship" limitation-at-issue, Petitioner relies on Stokes's edges modeling

“computer-to-computer connections or user logon events” and concludes that each edge corresponds to a relationship. Pet., 21-22. But, significantly, for dependent claim 2, Petitioner concedes that “*edges in Stokes represent events* (e.g., ‘computer connections and user logon events’),” not relationships, and argues that a sequence of those edges satisfies the claimed “event flows.” Pet., 37-38. And for claim 11, Petitioner similarly states that “Stokes describes representing network connection events as edges in a graph,” and relies on those edges to show that a “given event relates to particular entities represented in the graph.” *Id.*, 45.

Thus, when the claim requires a “relationship,” Petitioner treats Stokes’s connection-event edges as relationships; when the claim requires an “event,” Petitioner treats those same graph edges as events. Petitioner provides no principled explanation for how Stokes’s edges are both the claimed “events” and the claimed “relationships.” Petitioner’s unsupported and inconsistent assertions cannot satisfy Petitioner’s burden. *Engel*, 96 F.3d at 1405 (separately recited “second portion” and “return portion” “logically cannot be one and the same”).

Petitioner cites its expert, Dr. Black, but his declaration is equally conclusory and substantially repeats the Petition. *Compare* Pet., 21-22 with Ex. 1003 [Black Decl.] ¶ 81. He never, however, provides an explanation of *why* an event is a relationship, particularly when the claim language and the specification confirm otherwise. *See* Section II.A.1.

It is well-settled that an expert's conclusory statements are insufficient to establish unpatentability. *See* 37 C.F.R. § 42.65(a) (unsupported expert testimony entitled to "little or no weight"); *see also Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 887 n.2 (Fed. Cir. 2024) ("the conclusory assertions in Dr. Mohazzab's declaration do not provide substantial evidence for finding a motivation to combine.").

This is particularly so where, as here, the expert merely repeats the Petition's conclusions. As the Board held in *Xerox*:

Petitioner's only evidence in support of its assertion that blocking the purchaser would require recording the blocking in a record in the user's account is the opinion of its Declarant, Dr. Jones. ... Dr. Jones does not cite to any additional supporting evidence or provide any technical reasoning to support his statement. Thus, the cited declaration testimony is conclusory and unsupported, adds little to the conclusory assertion for which it is offered to support, and is entitled to little weight.

Xerox Corp. v. Bytemark, Inc., IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential). The same is true here. The cited Stokes passages establish that its individual edges record events. Dr. Black supplies no technical reasoning establishing that those events are the claimed relationships.

b. *Stokes's Individual Event Records Do Not Establish The Claimed Relationships.*

Petitioner's mapping turns on what Stokes's individual edges represent.

Petitioner first relies on Stokes's "computer-to-computer connections or user logon *events*" as the individual edges.¹ Pet., 21-22. But Stokes repeatedly characterizes those edges as records of particular events, as Petitioner acknowledges. Pet., 37-38 ("edges in Stokes represent events"); Ex. 1003 [Black Decl.] ¶ 122 ("edges in Stokes represent events"). As Dr. Malek explains:

Stokes repeatedly characterizes its mapped edges as records of particular network events or connections, rather than as relationship information of the type recited in the '627 claims. Stokes explains that "edges indicate network connection *events* such as a user logging onto a computer or a computer connecting to another computer," and that "[e]ach Kerberos record represents an edge in the graph, with a source

¹ Petitioner's own claim 11 mapping confirms that "computer-to-computer connections" is being used here to refer to connection events, not a relationship. Petitioner expressly states that "Stokes describes representing network connection events as edges in a graph," and relies on those edges to show that an "event relates to particular entities represented in the graph." Pet., 45. Stokes likewise explains that each edge has a timestamp "indicating when this connection occurred." Ex. 1004 [Stokes] [0038].

node, a destination node, and *a timestamp indicating when this connection occurred.*” Ex. 1004 [Stokes] [0038]. Thus, in Stokes’s specific implementation, the edge is a record of an observed event or connection occurrence, including when it occurred. Stokes confirms that understanding throughout the disclosure. It describes “system and security *events*” used to build the graph and states that “network logon *events*” may also be used to implement the graph. *Id.*, [0050]-[0051]. Stokes’s “operational flow” likewise begins by generating the graph “using system and security *events*,” and then determines edge weights and path-rate scores from that event-based graph. *Id.*, [0057]-[0061].

Thus, Stokes’s specific edge disclosures characterize the mapped edges as time-stamped event or connection records. Standing alone, those event records do not identify the claimed relationship Petitioner contends is represented by Stokes’s edge.

Ex. 2003 [Malek Decl.] ¶¶ 51-52.

Nor do the particular event types Petitioner relies upon qualify as relationships. Petitioner identifies “computer-to-computer connections or user logon events.” Pet., 21. But Stokes identifies each of those items as events recorded in “event logs.” Ex. 1004 [Stokes] [0038]. In Stokes, these “connection events” identify what occurred at a particular moment in time; it does not identify what relationship exists between the entities. Indeed, that a login or connection occurred at one moment in time provides no indication of whether the login or connection exists at another point in time.

The examples make the deficiency concrete. The “network connection events such as a user logging onto a computer or a computer connection to another computer” record “a timestamp indicating when this connection *occurred*.” Ex. 1004 [Stokes] [0038]. In a system taught by the ’627 patent, such an event might provide evidence of, or result in an identification of a “HasSession” relationship, but the timestamp when the connection occurred and the resulting relationship are distinct. Ex. 2003 [Malek Decl.] ¶ 54. Petitioner never identifies which relationship it contends is represented by any of these events or explains why the occurrence itself is that relationship.

Stokes’s teachings are materially different from the ’627 patent’s. The ’627’s Figure 22, for instance, expressly identifies relationship information:

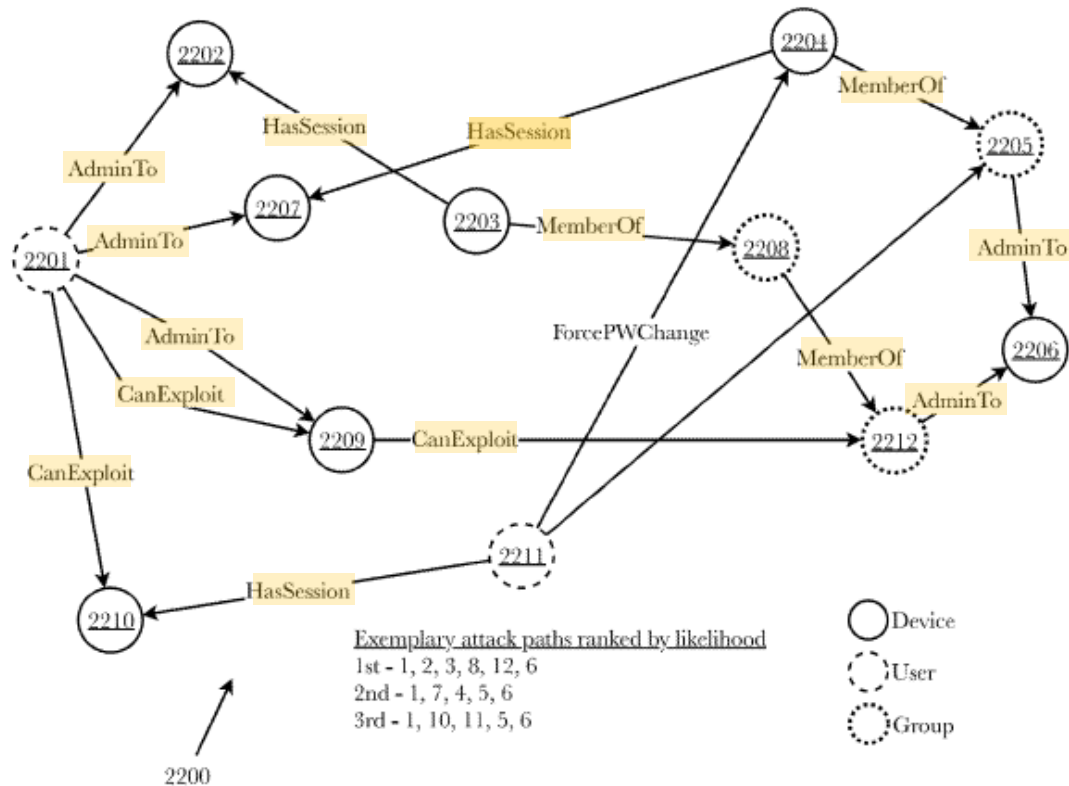


Fig. 22

Ex. 1001 [’627] Fig. 22 (annotated). As shown above, the Figure 22’s edges are expressly labeled with “relationship indicator[s]” such as “AdminTo,” “MemberOf,” “HasSession,” “CanExploit,” and “ForcePWChange.” *Id.*, Fig. 22, 28:41-42. Those indicators characterize how the represented entities are connected—for example, whether an entity administers another entity, is a member of a group, has a session with a device, or can exploit another entity. By contrast, Stokes identifies what event occurred, when it occurred, the source node, and the

destination node. It does not identify relationship information apart from the event record that Petitioner maps to the claim.

The point is not that the claims require the specific labels used in Figure 22. The point is that Figure 22 illustrates the relationship information described by the '627 patent. Stokes's edges, by contrast, are simply particular event occurrences; *e.g.*, a timestamp of when a login or connection occurred. Petitioner does not identify relationship information separate from the event record that Petitioner maps to the claim. Petitioner simply assumes that the two are the same.

Thus, Stokes's individual edges do what Stokes says they do: represent particular events. And this is undisputed. Petitioner and its expert concede that "edges in Stokes represent events." Pet., 37-38; Ex. 1003 [Black Decl.] ¶ 122. But Petitioner never explains why those event edges satisfy both the "event" *and* "relationship" limitations, nor identifies the specific relationship allegedly represented by any cited event type. Accordingly, Petitioner fails to prove that Stokes's event-edges establish the claimed relationships.

c. *Stokes's Generic Graph Statement Does Not Change The Fact That Stokes's "Edges Represent Events."*

Petitioner and Dr. Black also rely on Stokes's statement that "E" represents "the set of connection relationships ... between pairs of *nodes*, called edges." Pet., 21-22; Ex. 1003 [Black-Decl.] ¶ 81. But that general statement does not establish

what the Stokes's edges Petitioner relies upon represent. The question is not whether an edge could represent a relationship between nodes; the question is whether Stokes's particular mapped edges correspond to a relationship between entity pairs. And, as to the operative question, there is no dispute concerning what Stokes's edges represent. As Petitioner and Dr. Black concede, "edges in Stokes *represent events*." Pet., 37-38; Ex. 1003 [Black Decl.] ¶ 122.

Stokes teaches that it uses "graph concepts" to "model[]" "the lateral movement detection problem." Ex. 1004 [Stokes] [0038]. In its graph, "edges indicate network connection *events* such as a user logging onto a computer or a computer connection to another computer." *Id.* Stokes teaches that it can collect records representing edges in the graph from "*event* logs." *Id.* Each of these records have "a source node, a destination node, and *a timestamp indicating when this connection occurred*." *Id.*

The cited disclosures thus identify event records used as the edges of Stokes's graph: a source, a destination, and a timestamp reflecting when a logon event or connection event occurred. But Petitioner still does not identify the relationship allegedly corresponding to those event records or explain why the event occurrence itself is the claimed relationship. A generic statement that graph edges can reflect relationships does not explain why the edges Petitioner relies upon—which it concedes represent events—satisfy the claim requirement that each

edge corresponds to a respective relationship between a respective pair of entities.

Accordingly, Petitioner fails to demonstrate that Stokes's particular event records are the claimed relationships or that Stokes's edges to respective relationships between entity pairs. Petitioner therefore has not shown that Stokes teaches "wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities."

B. Petitioner Fails To Demonstrate That Stokes-Crabtree Discloses Or Renders Obvious The Claimed Attack Path Limitations (All Claims, All Grounds).

Petitioner's Stokes-Crabtree combination fails because the independent claims impose two related attack path requirements that Petitioner never satisfies. First, after the graph is modified to add a newly identified entity, the system must identify attack paths based on that modified graph and account for the newly added entity. Second, the claim language, specification, and prosecution history confirm that the attack path analysis identifies potential exposure in the graph—not computers or accounts already compromised by a prior attack/traversal. *See* Section II.B.1.

Stokes-Crabtree does not teach either requirement. Petitioner relies on Crabtree for graph updating, but relies on Stokes for the attack path analysis. Stokes starts with a node already identified as malicious or compromised, then uses graph paths to identify other already compromised computers and accounts.

Updating the graph with the streaming approach of Crabtree might give Stokes a newer map, but does not change Stokes's methodology. Stokes still starts with a compromised node and looks for other already compromised computers or accounts, rather than using a graph with edges that represent relationships between entities to identify a *potential* attack path. Stokes's search for already compromised nodes is precisely what the Applicant disclaimed during prosecution. *See* Section II.B.2.

After relying on Stokes's compromised-node investigation and Crabtree's graph updating, Petitioner asserts that the Stokes-Crabtree system "would apply that same path-identification analysis to a modified graph, including paths involving any newly added nodes." Pet., 32. But applying Stokes's "same" analysis to an updated graph does not cure either defect. Stokes would still start with a node already identified as malicious or compromised and use information about past events, identified by the edges of Stokes's graph, to find other already compromised computers or accounts. Petitioner and Dr. Black identify no reason why the combination would satisfy the claimed requirements. *See* Section II.B.3.

1. The Claims Require Identifying Attack Paths From The Newly Added Entity Before The Claimed Path Has Already Been Traversed.

The claim language and prosecution history establish two related requirements relevant here. First, the claimed attack path must be identified from

the modified graph and must involve the newly added entity. *See* Section II.B.1(a), *infra*. Second, the claimed attack path is a prospective path of potential compromise: the system identifies where an attack could proceed through the newly added entity, not which computers or accounts have already been compromised after an attacker laterally moved through the network. *See* Section II.B.1(b), *infra*.

- a. *The Claimed Attack Path Analysis Must Be Based On The Modified Graph And Must Involve The Newly Added Entity.*

Claim 1 requires identifying a first entity that was not represented in the original graph and modifying the graph to add a first node corresponding to that entity. Ex. 1001 [’627] cl. [1.7] (“identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities.”); [1.9] (“modify ... the representation of the first graph ... wherein the modified representation of the first graph comprises a representation of a first node corresponding to the first entity ...”). The claim then requires identifying, “based on the modified representation of the first graph,” an attack path that “could be involved in an attack involving the first entity.” *Id.*, cl. [1.10]. Identifying an attack path from the first entity entails identifying a second entity that “can be reached using the first entity,” and a third entity that “can be reached using the second entity.” *Id.*, [1.11].

Thus, the claimed attack path proceeds through the newly added first entity in the modified graph—an entity that was not in the first, unmodified graph—and proceeds through entities that can be reached in a path from that newly added entity. The claim is not satisfied by identifying a malicious path untethered to the newly added node, or by identifying compromised nodes somewhere else in the graph. The path must be identified from the modified graph and must involve the newly added first entity.

Claim 18 contains a similar modified-graph/newly added entity requirement, in analogous form. It requires modifying the graph to add a node corresponding to a newly identified third entity, and then identifying, based on the modified graph, a second plurality of attack paths where one attack path comprises that newly added third entity. Ex. 1001 [’627] cl. 18. Thus, for both challenged independent claims, the attack path limitation is tied to the modified graph with the newly identified entity as a node, and the attack path analysis must account for that newly added entity.

b. *The Claimed Attack Path Analysis Identifies Potential Exposure, Not Nodes Already Compromised By Prior Traversal.*

Claim 1 recites a path that “could be involved” in an attack and entities that “can be reached” along that path. Ex. 1001 [’627] cl. [1.10]-[1.11]. That language addresses *potential* compromise: what entities *could* be exposed if an attack

proceeds through the modified graph from the newly added entity.

In accord, the specification describes graph-based analysis of “possible attack paths,” ranking attack paths by likelihood, and predicting “what systems or resources might be at risk.” *Id.*, 25:3-21, 28:43-65. The attack path therefore identifies potential exposure in the graph; it is not merely a forensic report of where the attacker already went or which nodes are already compromised.

The prosecution history—and the Applicant’s disclaimers therein—confirms and, indeed, mandates that understanding. Following a rejection over a combination of the Neil and Altman references (Ex. 1002 [Pros. Hist.] 188-189), the Applicant amended the claims (*id.*, 220-229). In associated remarks, the Applicant distinguished Neil because Neil identified “where the attacker has already been in the network, in contrast to pending claim 1”:

The *Neil* system relies on the fact that, “as the attacker traverses the network, he or she creates anomalous activity in time series of communications along each edge that he or she traverses” and performs its detection by looking for a, “union of these anomalous edges in some interval of time” that were created as the attacker traversed the network. *Neil* at ¶ [34]. ***Thus, Neil focuses on types of statistical models that are used to identify where the attacker has already been in the network, in contrast to pending claim 1.***

Ex. 1002 [Pros. Hist.] 237-238.

The Applicant distinguished Altman for the same reason, explaining that Altman was “based on message traversal through the network *that has already happened.*” *Id.*, 238. The Applicant thus made a clear disclaimer, drawing a line between the claimed attack path analysis and prior-art systems that detect or reconstruct “where the attacker has already been in the network” or a “traversal ... that has already happened” with the latter falling outside of the scope of the claims.

Consistent with that distinction, the Examiner then amended claim 1 into its issued form, including the requirement to identify “an attack path that could be involved in an attack involving the first entity”:

identify, based on the modified representation of the first graph, an attack path that could be involved in an attack involving the first entity, wherein identifying the attack path comprises:

identifying a second entity that can ~~potentially be accessed~~ reached using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph; and,

identifying a third entity that can be reached using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph; and

generate a report comprising an identification of ~~at least one of~~ the first entity and at least one of the second entity and the third entity.

Id., 276. This amendment further cemented in the claim the distinction the Applicant drew. The Examiner allowed the claims on that same basis. In the Reasons for Allowance, the Examiner identified as missing from Neil and Altman

the requirement to “identify, based on the modified representation of the first graph, an attack path that could be involved in an attack involving the first entity,” including the requirements for identifying second and third entities that “can be reached” through the modified graph. *Id.*, 278-279.

The same prosecution-history distinction applies to claim 18. In the same remarks, the Applicant explained that new claim 27, which issued as claim 18, “recites similar features as pending claim 1,” and that “[c]laim 27 is allowable for similar reasons as claim 1, as explained in detail above,” referencing its argument under claim 1. *Id.*, 238. The Examiner agreed, finding claim 18 allowable over Neil/Altman. *Id.*, 279-280; Ex. 1001 [’627] cl. 18.

This record establishes prosecution disclaimer. The Applicant surrendered any interpretation under which the claimed attack path limitation is satisfied by detecting or reconstructing “where the attacker has already been in the network” or a “traversal ... that has already happened.” *See Ekchian v. Home Depot, Inc.*, 104 F.3d 1299, 1304 (Fed. Cir. 1997) (distinguishing the claimed invention over prior art indicates “what the claims do not cover” and surrenders that subject matter); *Spectrum Int’l, Inc. v. Sterilite Corp.*, 164 F.3d 1372, 1378 (Fed. Cir. 1998) (statements distinguishing prior art during prosecution may narrow claim scope); *Saffran v. Johnson & Johnson*, 712 F.3d 549, 559 (Fed. Cir. 2013) (applicants need not use formal “I hereby disclaim” language to create disclaimer).

The Examiner's amendment reinforces the Applicant's disclaimer. The Applicant first distinguished Neil and Altman because they identified where an attacker "has already been" or a traversal that "has already happened." Ex. 1002 [Pros. Hist.] 237-238. The Examiner then amended claim 1 into its issued form, including the requirement to identify "an attack path that could be involved in an attack involving the first entity," and allowed the claims because Neil and Altman did not disclose that limitation. *Id.*, 276, 278-80. That sequence confirms that the Applicant and the Office shared the same understanding of the amended claims. *See ACCO Brands, Inc. v. Micro Sec. Devices, Inc.*, 346 F.3d 1075, 1078-79 (Fed. Cir. 2003) (examiner's reasons for allowance confirmed that "the examiner and the applicant understood" what was changed and what the invention required).

At a minimum, even if the Director were to conclude that Applicant's statements do not rise to the level of disclaimer, the prosecution history confirms the proper understanding of the claim language. *See D'Agostino v. MasterCard Int'l Inc.*, 844 F.3d 945, 949 (Fed. Cir. 2016) (prosecution statements distinguishing the invention from the prior art may reinforce "the evident meaning of the claim language," even if they do not meet the standard for disclaimer).

The claims, thus, require identifying a potential attack path involving the newly added entity in the modified graph. Those limitations are not satisfied by an attack path analysis that merely determines what computers/accounts have already

been compromised.

2. Petitioner's Stokes-Crabtree Theory Does Not Satisfy Either Claim Requirement.

As just explained, the independent claims impose two related requirements. First, the challenged attack path analysis must be based on the modified graph and must account for the newly added entity. Second, the attack path analysis identifies potential exposure in the graph; it does not cover using graph paths merely to determine which computers or accounts have already been compromised. *See* Section II.B.1.

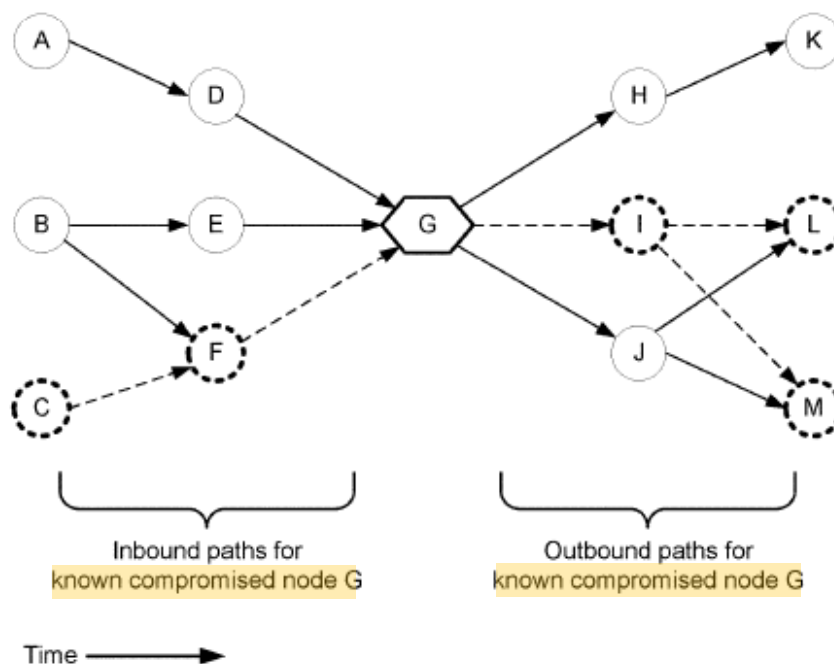
Petitioner's Stokes-Crabtree combination fails both requirements. Petitioner relies upon Stokes's attack path analysis, but the Stokes forensic analysis Petitioner invokes does not proceed because a new entity has been added to the modified graph. It starts from a computer or account already identified as malicious or compromised, and then analyzes paths into and out of that compromised node to find other compromised computers or accounts. Crabtree may update the graph, but it does not change what Petitioner relies on Stokes to do.

For limitation [1.10], Petitioner says Stokes identifies lateral movement “by first identifying a malicious node and then analyzing inbound and outbound paths from that node.” Pet., 30. Petitioner also relies on Stokes's statement that, “given a malicious node,” Stokes identifies “possible lateral movement leading into or out

of the node” and identifies “*other compromised computers.*” *Id.*; Ex. 1004 [Stokes] [0028].

Thus, Stokes’s starting point for its forensic analysis is a node already known or identified to be malicious or compromised. Stokes does not teach performing its forensic analysis for a node that was selected because it was newly added to the modified graph. As Dr. Malek explains:

Stokes’s Figure 3, which Petitioner relies upon (Pet., 31-32), illustrates determining paths for a “*known* compromised node”:



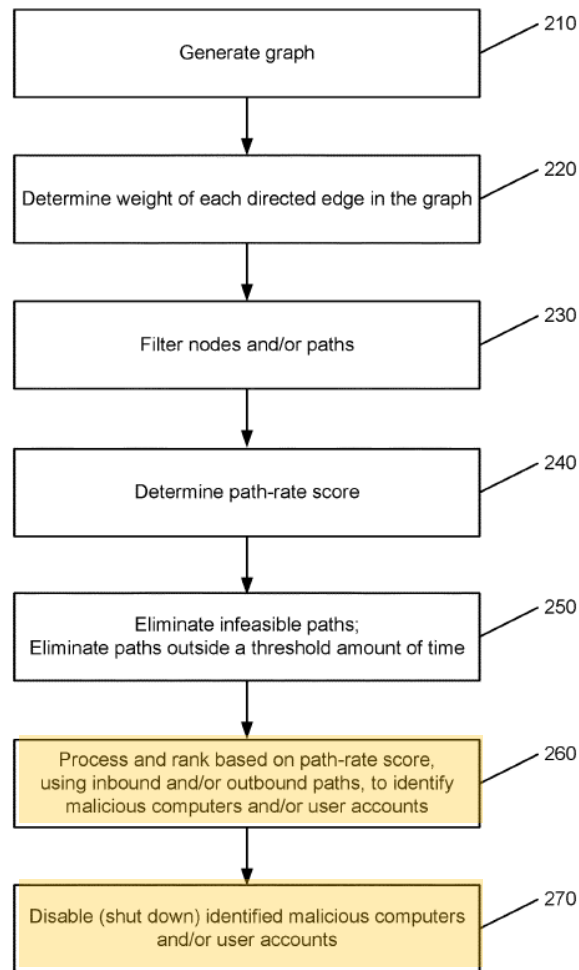
300

FIG. 3

Ex. 1004 [Stokes] Fig. 3 (annotated). Figure 3 does not depict an analysis triggered by adding a newly discovered entity to the graph. Instead, it begins with node G, which Stokes already “know[s]” is compromised, and then “identif[ies] the unknown compromised computers and user accounts (dashed nodes C, F, I, L, M) along the malicious access path (dashed lines).” *Id.*, [0066].

Ex. 2003 [Malek Decl.] ¶ 77.

That same Stokes disclosure also fails the second requirement. Petitioner relies on Stokes to identify “other compromised computers.” Pet., 30; Ex. 1004 [Stokes] [0028]. Stokes Figure 2 likewise processes and ranks paths “to identify malicious computers and/or user accounts,” and then disables those identified malicious computers or accounts:



200

FIG. 2

Ex. 1004 [Stokes] Fig. 2. Stokes Figure 3 identifies “unknown compromised computers and user accounts” along a “malicious access path.” *Id.*, [0066]. Those disclosures are about finding computers or accounts that have already been compromised, after the network has been traversed. They are not about identifying where an attack could proceed involving the newly added entity so that exposed entities can be identified before that path is traversed. As Dr. Malek explains:

Stokes is directed toward “detecting malicious lateral movement across a computer network.” Ex. 1004 [Stokes] Title. The Stokes forensic analysis Petitioner relies upon begins “given a malicious node” and identifies possible lateral movement into or out of that node to identify “other compromised computers.” *Id.*, [0028]. Stokes’s Figure 3 likewise begins with “known compromised node G” and identifies unknown compromised computers and user accounts along a malicious access path. *Id.*, Fig. 3, [0066]. Thus, although Stokes uses the phrase “possible lateral movement,” Stokes’s forensic analysis uses those paths to find other compromised computers or accounts. When Stokes discusses “malicious lateral movement,” therefore, Stokes is referring to events that have already happened or are happening. Stokes does not disclose the claimed post-modification attack path analysis involving the newly added entity.

Ex. 2003 [Malek Decl.] ¶ 79.

That is the same distinction the Applicant made during prosecution. Again, the Applicant distinguished Neil because Neil identified “where the attacker has already been in the network,” and distinguished Altman because it was based on traversal that “has already happened.” Ex. 1002 [Pros. Hist.] 237-238. Stokes falls on the same side of that line. It starts with a compromised node and uses graph paths to identify other already compromised computers or accounts. The fact that Stokes calls those paths “possible lateral movement” does not change what Stokes uses them for: finding other compromised nodes.

Crabtree does not cure either defect. Petitioner relies on Crabtree for graph updating. *See* Pet., 23-30. But for limitation [1.10], Petitioner relies on Stokes's analysis. *See id.*, 30-34. At most, Crabtree gives Petitioner a more current graph. It does not change Stokes from an investigation that starts with a compromised node and finds other already compromised computers or accounts into the claimed forward-looking attack path analysis involving the newly added entity.

The prosecution history reinforces the point. During prosecution, the Examiner had already combined Neil's graph-based attack/anomaly detection with Altman's graph modification, including adding nodes and edges. Ex. 1002 [Pros. Hist.] 189-192. The Applicant still overcame the rejection because the attack path theory rested on traversal that had already occurred. *Id.*, 237-238. Petitioner's Stokes-Crabtree theory has the same problem. Crabtree updates the graph, but Petitioner still relies on Stokes to identify other already compromised computers or accounts.

The same two defects apply to claim 18. Claim 18 requires identifying, based on the modified graph, a second plurality of attack paths where one attack path comprises the newly identified third entity. Ex. 1001 ['627] cl. 18. Petitioner does not identify such a disclosure in Stokes. Instead, Petitioner asserts that "once the modified graph includes a node representing the third entity," a POSITA "would have applied Stokes's path analysis to that modified graph," and then

presents a modified version of Stokes Figure 3 that adds new node N and new G-N and N-M edges. Pet., 58-61, 60 n.6. That confirms the first defect: the newly added third entity appears only in Petitioner's modified figure, not in Stokes. The Petition states that the modified Figure 3 "adds new node N and new black dashed lines to represent the G-N edge and N-M edge," and that "[n]ew node N represents the type of node that would be added to the graph." Pet., 60-61, 60 n.6. Those additions are Petitioner's hypothetical, not Stokes's disclosure.

Petitioner's claim 18 theory also confirms the second defect. Petitioner says the newly added third entity/node may correspond to an "unknown compromised computer or user account," and that the modified graph would reflect a malicious actor "exploring and accessing multiple resources." Pet., 59-60. The modified Figure 3 then remains built around Stokes's same already-compromised-node investigation. *Id.*, 60-61. Here too, Petitioner does not identify potential exposure involving the newly added entity; just a backwards-looking forensic analysis to determine what was already corrupted of the very kind disclaimed in prosecution.

Accordingly, Petitioner fails to show that Stokes-Crabtree teaches the challenged attack path limitations. Stokes starts with a compromised node and looks for other already compromised computers or accounts. The claims require an attack path analysis involving the newly added entity and identifying potential exposure in the modified graph. Crabtree's graph updating does not cure that

mismatch.

3. Petitioner Cannot Fill The Gap With Unsupported “Obvious Use Case” Testimony.

Sections II.B.1-II.B.2 show why Petitioner’s Stokes-Crabtree theory fails.

Stokes starts with a computer or account already identified as malicious or compromised, then uses graph paths to find other computers or accounts that are also already compromised. Crabtree may update the graph, but updating the graph does not change what Stokes does. Petitioner still had to explain why the combined system would do what the claims require: using the modified graph to identify an attack path involving the newly added entity and the entities that could be exposed along that path. The Petition provides no such explanation for why the Stokes-Crabtree combination would satisfy the claims.

Instead, it simply asserts that Stokes’s same path-identification analysis “would apply” to a modified graph “including paths involving any newly added nodes.” Pet., 32. Petitioner argues:

The Stokes-Crabtree system *would apply* that same path-identification analysis to a modified graph, *including paths involving any newly added nodes*. For example, where the modified graph includes a newly added node corresponding to a first entity (*e.g., supra* Sections VII.D.7-9) that is *potentially* malicious, Stokes’s forensic analysis would identify the dashed paths of Figure 3 as attack paths involving that first entity. EX1003, ¶110; *see also* EX1004, [0045],

[0048]. In the combined Stokes-Crabtree system, with Crabtree’s teachings on modifying the graph to add new nodes for new entities, identified attack paths would involve new entities not represented in the initial graph (additional examples of *first entities*). EX1003, ¶110.

Id., 32-33.

We are told Stokes-Crabtree “would” do this, but we are not told why. Neither Stokes nor Crabtree discloses using the modified graph to identify a not yet traversed attack path involving the newly added entity. Stokes analyzes paths from a node already identified as malicious or compromised to find other compromised computers or accounts. Crabtree updates the graph. Neither reference discloses using the modified graph to identify potential attack paths involving the newly added entity so that other entities exposed along those paths can be identified. Petitioner simply asserts that the combined system “would apply” Stokes’s path-identification analysis to a modified graph “including paths involving any newly added nodes.” *Id.*, 32.

To the extent Petitioner relies on Dr. Black’s undeveloped “obvious use case” scenarios to supply the missing reasoning, that is improper incorporation by reference. *See* Pet., 32-33 (citing but not discussing paragraph 110 of the Black declaration). The Petition itself had to make the argument. *See* 37 C.F.R. § 42.6(a)(3) (“Arguments must not be incorporated by reference from one document

into another.”); *Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12, 9-10 (Aug. 29, 2014) (informative) (finding improper incorporation where the petition relied on conclusory statements and cited an expert declaration for the supporting argument). Thus, Dr. Black’s testimony should not be considered.

But even if Dr. Black’s paragraph is considered, it is equally unsupported and conclusory. He does not identify where Stokes or Crabtree discloses using the modified graph to identify the not yet traversed attack path involving the newly added entity. He instead labels the missing step an “obvious use case,” invoking the phrase three times in a single paragraph:

As explained above for elements [1.7] and [1.9], Sections VIII.D.7 and VIII.D.9 *above*, Stokes-Crabtree teaches identifying a new first entity and modifying the graph to include a first node corresponding to that first entity. EX1004, [0048], [0066]-[0071]. *A POSITA would have recognized an obvious use case* in which the Stokes-Crabtree combination identifies a malicious path (i.e., attack path) based on the modified graph, and where the identified attack path involves the first entity. For example, *a POSITA would have recognized an obvious use case* in which compromised node G (highlighted above) corresponds to an entity not represented in the initial graph, and the Stokes-Crabtree system identifies the red dashed paths of annotated Figure 3, above, as attack paths involved in an attack involving the entity that corresponds to compromised node G (i.e., the first entity). Such use cases include a known malicious entity or a

computer or account included in Stokes's "compromised computer and account list" newly accessing the network or the known compromised node otherwise having been newly added to the graph (for example for not having been previously accessed within the relevant time period for the graph). EX1004, [0045], [0048]. *A POSITA would understand that in other obvious use cases*, identified attack paths would be involved in attacks involving other entities, such as an entity which corresponds to another node of Figure 3 and was not represented in the initial graph.

Ex. 1003 [Black Decl.] ¶ 110.

Dr. Black's paragraph thus identifies three supposed "obvious use case[s]." First, he posits that Stokes's compromised node G could be the newly added first entity. *Id.* Second, he posits that a known malicious entity, or a computer or account already on Stokes's "compromised computer and account list," might newly access the network or otherwise be newly added to the graph. *Id.* Third, he posits that some other node in Stokes Figure 3 could be an entity not represented in the initial graph. *Id.* None of those hypothetical scenarios is disclosed in Stokes or Crabtree. And none explains why the combined system would use the modified graph to identify other entities that may be threatened, rather than use Stokes's ordinary compromised-node analysis to find other already compromised computers or accounts. A claimed use case is not "obvious" merely because an expert so asserts.

At most, Dr. Black posits scenarios in which Stokes's compromised node G, a known malicious entity, or another Figure 3 node might just so happen to be newly added to the graph. That is not enough. A possibility that the prior art might satisfy a limitation by happenstance is not sufficient. *See In re Facebook, Inc.*, 743 F. App'x 998, 1001-02 (Fed. Cir. 2018) (nonprecedential) (prior-art example that "happened to result" in the claimed arrangement did not teach the limitation where the prior-art algorithm did not require that result); *In re Felton*, 484 F.2d 495, 500 (C.C.P.A. 1973) ("it would be mere happenstance" if the prior-art structure met the claim limitations, which was insufficient for anticipation or obviousness); *Bettcher Indus., Inc. v. Bunzl USA, Inc.*, 661 F.3d 629, 640 (Fed. Cir. 2011) ("speculative notion" that the prior art might, "by happenstance," operate as claimed under hypothetical circumstances was insufficient). Here, nothing in Stokes or Crabtree teaches the modified graph to identify a potential attack path involving the newly added entity. Dr. Black simply assumes that Stokes's compromised-node analysis may satisfy the claims if the compromised node just happens to be newly added.

Dr. Black provides no objective support for those scenarios. He does not identify any prior-art reference, industry publication, commercial system, technical standard, or contemporaneous example showing that any of those use cases was known. Nor does he explain why a POSITA would use the newly added entity in

the claimed attack path analysis rather than simply run Stokes's ordinary analysis from a node already identified as malicious or compromised. He simply labels the scenarios "obvious use case[s]."

Dr. Black's Stokes citations do not supply the missing link. Paragraphs [0066]-[0071] concern Stokes's Figure 3/Figure 4 analysis rooted in a known compromised node G, inbound and outbound paths thereto which results in the identification of other compromised computers or accounts. Ex. 1004 [Stokes] [0066]-[0071]; *see also* Section II.B.2. Paragraph [0048] confirms that the forensic-analysis module receives a "compromised computer and account list." *Id.*, [0048]. Paragraph [0045] concerns path timing and timestamps. None disclose Dr. Black's scenarios: a compromised node G newly added to the graph, a known malicious entity newly accessing the network, or another Figure 3 node newly added and used in the claimed attack path analysis. Those are Dr. Black's *ex post facto* hypothetical scenarios, not Stokes's disclosures.

Petitioner's reliance on Dr. Black's *ipse dixit* is legally insufficient. Obviousness requires articulated reasoning supported by evidence, not a conclusory assertion that the missing limitation would have been an obvious use case. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (obviousness requires "some articulated reasoning with some rational underpinning"); *In re Magnum Oil Tools Int'l, Ltd.*,

829 F.3d 1364, 1380 (Fed. Cir. 2016) (a petitioner “cannot employ mere conclusory statements” and must provide “specific reasoning, based on evidence of record”). And it is well-settled that an expert’s conclusory statements are insufficient to establish invalidity. *See* 37 C.F.R. § 42.65(a) (unsupported expert testimony entitled to “little or no weight”); *see also Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 887 n.2 (Fed. Cir. 2024) (“the conclusory assertions in Dr. Mohazzab’s declaration do not provide substantial evidence for finding a motivation to combine.”).

The Board’s precedential *Xerox* decision is on point. There, the Board gave little weight to expert testimony where the declarant “does not cite to any additional supporting evidence or provide any technical reasoning to support his statement.” *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022) (precedential). The same is true here. Dr. Black does not cite evidence showing that it was known or obvious to use Stokes’s forensic analysis in the claimed way—*i.e.*, after adding a new entity to the graph, to identify the claimed attack path involving that newly added entity. He simply labels the missing scenario an “obvious use case.”

Petitioner’s “obvious use case” theory is also an improper attempt to use common sense to supply a missing limitation. The Federal Circuit has repeatedly warned that common sense cannot substitute for reasoned analysis and evidence,

especially when supplying a claim limitation missing from the prior art:

In cases in which “common sense” is used to supply a missing limitation ... ***our search for a reasoned basis for resort to common sense must be searching. And, this is particularly true where the missing limitation goes to the heart of an invention.***

Arendi S.A.R.L. v. Apple, Inc., 832 F.3d 1355, 1362-63 (Fed. Cir. 2016); *see also DSS Tech. Mgm’t v. Apple Inc.*, 885 F.3d 1367, 1374-75 (Fed. Cir. 2018) (rejecting “ordinary creativity” as a basis for overcoming a missing limitation); *K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1366 (Fed. Cir. 2014) (“Because [the appellant] failed to cite any evidence on the record to support claims 3 and 9 were known prior art elements, we affirm the Board’s decision to refuse to adopt [the appellant’s] obviousness contention.”).

The missing limitation is central to the challenged claims. The prosecution history confirms that the modified-graph attack path limitations were the basis for allowance over Neil and Altman. Ex. 1002 [Pros. Hist.] 235-238, 278-280. And the ’627 patent explains that understanding an organization’s cybersecurity profile is complex, with complexity increasing as network size grows. Ex. 1001 [’627] 2:34-44. This is not a simple, peripheral feature that can be supplied by unsupported “common sense.” Ex. 2003 [Malek Decl.] ¶ 92.

Dr. Black’s “obvious use case” theory is also hindsight-driven. For claim 1, he takes Stokes’s Figure 3, treats compromised node G—or another Figure 3 node—as the newly added entity, and declares that scenario obvious. For claim 18, Petitioner and Dr. Black go further: they add node N and new G-N and N-M edges to Stokes Figure 3 so that the modified figure contains the claimed newly identified third entity. Pet., 60-61, 60 n.6; Ex. 1003 [Black Decl.] ¶¶164-166. Stokes’s Figure 3 has no node N, no G-N edge, and no N-M edge. Petitioner and Dr. Black add those features because claim 18 requires an attack path comprising the newly identified third entity.

These are not examples from the prior art. They are reconstructions of Stokes’s Figure 3 using the claims as a template. For claim 1, Dr. Black substitutes the newly added first entity for compromised node G or another Figure 3 node. For claim 18, Petitioner and Dr. Black draw a new node and new edges into Figure 3. That is not evidence that Stokes or Crabtree taught the claimed structure; it is hindsight. *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 165 (Fed. Cir. 2021) (“The inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight.”) (quoting *Otsuka Pharm. Co., v. Sandoz, Inc.*, 678 F.3d 1280, 1296 (Fed. Cir. 2012)); *InTouch Techs., Inc. v. VGo Commc’ns., Inc.*, 751 F.3d 1327, 1351 (Fed. Cir. 2014) (rejecting expert’s obviousness theory that “relied on the [] patent itself as her roadmap for putting

what she referred to as pieces of a ‘jigsaw puzzle’ together.”); *In re Conrad*, 759 Fed. App’x. 982, 985-86 (Fed. Cir. 2019) (obviousness requires “a specific” rationale to combine limitations to make the claimed invention that is “*unrelated to* the rationale behind the *inventor’s* reasons for making the *[claimed]* invention.”).

Even accepting Dr. Black’s hypothetical scenarios, they still do not describe the claimed structure. His examples begin with a “compromised node,” a “known malicious entity,” or a computer or account already appearing on Stokes’s “compromised computer and account list.” Ex. 1003 [Black Decl.] ¶ 110. The scenarios merely change when the compromised node is added to the graph. They do not transform Stokes’s identification of already compromised nodes to an attack path that identifies not yet compromised nodes.

Accordingly, Petitioner fails to show that Stokes-Crabtree teaches limitation [1.10] or the analogous claim-18 attack path limitation.

III. CONCLUSION

Thus, Petitioner fails to demonstrate a reasonable likelihood of success as to any of the challenged claims and the Petition should be denied.

Respectfully submitted,

/ Kenneth J. Weatherwax /
Kenneth J. Weatherwax (Reg. No. 54,528)
Nathan Lowenstein, *pro hac vice*
Colette Woo, *pro hac vice*
LOWENSTEIN & WEATHERWAX LLP

Date: July 10, 2026

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Preliminary Response (the “POPR”) consists of 9,424 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POPR complies with the type-volume limitation of 14,000 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Respectfully submitted,

/ Michael Cosley /

Michael Cosley

Date: July 10, 2026

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served
by electronic service, by agreement between the parties, on the date below:

PATENT OWNER'S PRELIMINARY RESPONSE

EXHIBITS 2003-2005

The names and addresses of the parties being served are as follows:

Andrew M. Mason
Frank Morton-Park
Todd M. Siegel
Samuel B. Thacker

andrew.mason@klarquist.com
frank.morton-park@klarquist.com
todd.siegel@klarquist.com
samuel.thacker@klarquist.com
Msft-Qomplx@klarquist.com

Respectfully submitted,

/ Michael Cosley /

Michael Cosley

Date: July 10, 2026