

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

QOMPLX LLC,
Patent Owner.

Case IPR2026-00326
Patent 12,301,628

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. RELEVANT TECHNOLOGICAL BACKGROUND	3
A. The '628 Patent.	4
B. Brezinski.....	6
III. PETITIONER’S ONLY GROUND FAILS (ALL CLAIMS).....	8
A. Petitioner Fails To Show That Brezinski Teaches A “Relationship Between A Respective Pair Of Entities” (All Claims).	8
1. The '628 Patent Confirms That “Relationship[s]” And “Event[s]” Are Distinct.....	9
2. Petitioner Fails To Prove That Brezinski’s Events Are The Claimed Relationships.	16
a. Petitioner And Dr. Black Provide No Reasoned Basis To Conclude That Events Are Relationships.....	19
b. Brezinski’s Individual Event Records Do Not Establish The Claimed Relationships.....	22
c. Even Assuming Brezinski’s Events Were Relationships, Petitioner Fails To Show A Relationship That “Does Not Correspond To Any” First-Plurality Edge.....	27
d. Brezinski’s Generic Graph Definition Does Not Fill The Gap.....	31
B. Petitioner Fails To Demonstrate That Brezinski Teaches “Perform A First Correlation ... To Identify A First Plurality Of Correlated Nodes” (All Claims).....	33

IV. CONCLUSION.....	43
----------------------------	-----------

TABLE OF AUTHORITIES

	Page(s)
COURT DECISIONS	
<i>Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.</i> , 533 F.3d 1362 (Fed. Cir. 2008)	10
<i>Becton Dickinson & Co. v. Tyco Healthcare Grp., LP</i> , 616 F.3d 1249 (Fed. Cir. 2010)	10, 11, 30
<i>Engel Indus. v. Lockformer Co.</i> , 96 F.3d 1398 (Fed. Cir. 1996)	11
<i>Gaus v. Conair Corp.</i> , 363 F.3d 1284 (Fed. Cir. 2004)	10
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006)	20
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	21, 37
<i>Innova/Pure Water, Inc. v. Safari Water Filtration Sys.</i> , 381 F.3d 1111 (Fed. Cir. 2004)	30
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	20, 37
<i>Magnolia Med. Techs., Inc. v. Kurin, Inc.</i> , 169 F.4th 1094 (Fed. Cir. 2026)	11
<i>Virtek Vision Int’l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	21, 38

AGENCY DECISIONS

Xerox Corp. v. Bytemark, Inc.,
IPR2022-00624, Paper 9 (Aug. 24, 2022)
(precedential) 22, 38

REGULATIONS

37 C.F.R. § 42.65(a)..... 21, 37

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.
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 sole ground fails for two independent reasons.

First, Petitioner fails to demonstrate that Brezinski teaches the claimed "relationship[s]" between entity pairs. Petitioner's mapping depends on equating Brezinski's disclosed *events* with the claimed *relationships*. But Petitioner never even attempts to justify that false equivalence. In fact, "events" and "relationships" are different claim terms that play different roles: data about events is received, while relationships are identified "based on" that data. *See* Section III.A.1.

Ignoring that distinction in the intrinsic record, Petitioner simply asserts that Brezinski's events are "relationships." Petitioner never identifies the alleged relationship, never explains why Brezinski's event records supposedly satisfy the relationship limitations, and never demonstrates that any alleged relationship corresponding to a newly added event edge "does not correspond to any of the first plurality of edges." Moreover, Petitioner's own later mapping only confirms the disconnect: when addressing limitations that recite "events," Petitioner treats the same Brezinski edges as events rather than relationships. Petitioner provides no explanation for how Brezinski's events can qualify as both the claimed "events"

and the claimed “relationships.” Events are events—they are not relationships.

And, moreover, even if we were to assume, *arguendo*, that Brezinski’s events are relationships, Petitioner still fails to show that a newly added event edge in Brezinski “does not correspond to any of the first plurality of edges.” *See* Section III.A.2.

Second, Petitioner independently fails to demonstrate that Brezinski teaches “perform[ing] a ***first correlation*** ... to identify a first plurality of correlated nodes.” Petitioner does not rely on Brezinski’s disclosures that expressly discuss correlating events to generate its graph. And for good reason; Brezinski’s correlation does not satisfy the claims. Instead, Petitioner relies on Brezinski’s later graph-traversal and graph-element-selection disclosures, asserting that traversing the graph and identifying graph elements associated with anomalous activity performs the claimed correlation. But Petitioner never explains why those separately disclosed operations constitute the claimed “first correlation,” instead simply characterizing the identified nodes as “correlated.” *See* Section III.B.

Abraham Lincoln is said to have asked how many legs a calf would have if its tail were called a leg. The answer was four, because calling a tail a leg does not

make it one.¹ So too here. Calling Brezinski’s events “relationships” does not make them relationships, and calling Brezinski’s graph traversal a “correlation” does not make it one. Labels do not supply missing claim limitations. Because Petitioner fails to demonstrate a reasonable likelihood of prevailing, the Director should deny institution.

II. RELEVANT TECHNOLOGICAL BACKGROUND

The disputes at hand turn on two aspects of Petitioner’s graph-based mappings. The first concerns what the graph edges represent: the ’628 patent describes graph edges as representing relationships between entities, while treating event data as information that may be received, logged, and used to update or analyze the graph. Brezinski, by contrast, arranges event records into a graph whose individual edges correspond to events.

The second concerns what operation is performed using the graph. The claims require performing a “first correlation” using the modified graph to identify correlated nodes. Petitioner maps that limitation to Brezinski’s graph traversal and selection of graph elements for anomalous activity data. But Brezinski describes,

¹ [Lincoln quote sourced: Calf’s tail, not dog’s tail | Millard Fillmore’s Bathtub](https://timpanogos.blog/2007/05/23/lincoln-quote-sourced-calfs-tail-not-dogs-tail/) (available at <https://timpanogos.blog/2007/05/23/lincoln-quote-sourced-calfs-tail-not-dogs-tail/>).

separately, generating a graph that correlates events and traversing that graph to identify anomalous activity. That distinction provides context for Petitioner's reliance on Brezinski's traversal as the claimed correlation.

A. The '628 Patent.

The '628 patent concerns, *inter alia*, “correlating network event anomalies” to identify attack information. Ex. 1001 ['628] Title. The patent describes maintaining “an up-to-date model of the network in real time” in the form of a graph (*id.*, 26:6–8), identifying correlations between anomalous events and other network resources represented in the graph, and ascertaining attack pathways from those correlations. *Id.*, Abstract; Ex. 2003 [Malek Decl.] ¶ 34.

The '628 patent uses graph-based representations to model cybersecurity information. Generically, as a matter of mathematical definition, graphs consist of “nodes” (sometimes called “vertices”) and edges, each of which connects a pair of nodes. Ex. 1001 ['628] 7:47–51. In the '628 patent's specific graphs, an edge between two nodes represents the relationship between the entities those nodes represent. *Id.*, 3:18–20. For example, the edge between two nodes representing a pair of people may indicate that the two people know each other. *Id.*, 7:51–60; Ex. 2003 [Malek Decl.] ¶ 35.

Further examples of such relationships in the context of the '628's claimed graph are shown, *e.g.*, in Figure 22 which illustrates relationship edges labeled

“AdminTo,” “MemberOf,” “HasSession,” “CanExploit,” and “ForcePWChange.”

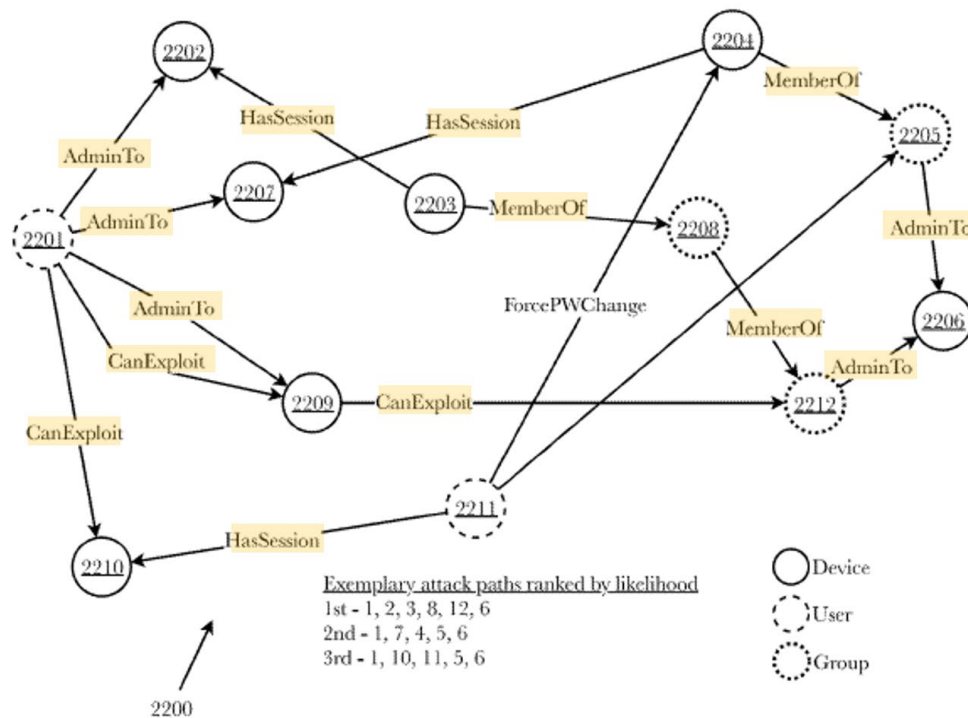


Fig. 22

Ex. 1001 [’628] Fig. 22; *id.*, 28:42–45. The specification explains that “[t]he edges (lines) between the nodes indicate relationships between the nodes, and have a direction and relationship indicator such as ‘AdminTo,’ ‘MemberOf,’ etc.” *Id.*, 28:42–45; Ex. 2003 [Malek Decl.] ¶ 36.

The ’628 patent also describes event information as data that is further processed to update and analyze the graph. Figure 11 depicts receiving “time-series event data” and then producing a “visualization of physical and logical relationships based on all received data types.” Ex. 1001 [’628] Fig. 11. The accompanying description explains that time-series information is “received and

incorporated, updating CPG information as changes occur and events are logged,” and that the resulting graph visualization correlates physical and logical relationships to reflect “the current state of the internal relationships present in the infrastructure.” *Id.*, 24:5–16; Ex. 2003 [Malek Decl.] ¶ 37.

Finally, the claims reflect this architecture. Claims 1 and 11 recite graph edges corresponding to relationships between entity pairs, receiving streaming data comprising time-stamped data about events, identifying a relationship based on that event data, and later performing a “first correlation” using the modified graph to identify correlated nodes. Ex. 1001 [’628] cls. 1, 11; Ex. 2003 [Malek Decl.] ¶ 38.

B. Brezinski.

Brezinski describes collecting event data from host devices and arranging that event data into a graph for later analysis. Ex. 1004 [Brezinski] Abstract. The event data describes events that have already occurred involving accesses or interactions between entities such as host devices, processes, or services. *Id.*, 2:14–30. Each event description may identify the initiating entity, the target entity, a timestamp, an event type, a user identifier, and other attributes. *Id.*, 5:65–6:10, 6:37–44; Ex. 2003 [Malek Decl.] ¶ 39.

Brezinski generates graph 118 from that event data. Vertices 402 correspond to entities, while individual edges 404(1) “each correspond to a

particular event.” Ex. 1004 [Brezinski] 8:29–40. Each individual edge may include attributes of a past event, such as timestamp, event type, user, and risk metric. *Id.*, Fig. 4; *id.*, 8:63–9:5. Brezinski also contemplates multiple individual edges between the same pair of vertices when multiple past events involve the same pair of entities. *Id.*, 8:43–52. Separately, overlay edges 404(2) may summarize graphed events of a particular type connecting a pair of vertices. *Id.*, 8:40–42, 9:55–10:4; Ex. 2003 [Malek Decl.] ¶ 40.

Brezinski also distinguishes generating the graph from later analyzing it. It describes determining a graph that “correlates a plurality of events” and, separately, “identifying anomalous activity by traversing the graph” according to rarity and risk metrics. Ex. 1004 [Brezinski] 2:8–13; *see also id.*, 2:31–32, 8:23–27. As discussed in Section III.B, *infra*, Petitioner relies upon Brezinski’s traversal not its correlation. Figure 10 depicts the graph-generation process, including determining a graph with vertices associated with entities and edges corresponding to events between the entities. *Id.*, Fig. 10; 16:15–36. Figure 11 depicts a later process for accessing the graph, traversing edges, and including qualifying edges and connected vertices in anomalous activity data. *Id.*, Fig. 11; *see also id.*, 17:39–18:44. Brezinski also permits additional criteria for including graph elements in anomalous activity data, such as interactions with a honey pot entity. *Id.*, 12:35–53; Ex. 2003 [Malek Decl.] ¶ 41.

III. PETITIONER’S ONLY GROUND FAILS (ALL CLAIMS).

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

The claims impose two relationship requirements. First, 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* of the first plurality of entities.” Ex. 1001 [’628] cls. 1, 11.

Second, after receiving “streaming data comprising time-stamped data about events,” the system must, based on a second portion of that streaming data, “*identify a first relationship between a pair of entities*” that “*does not correspond to any of the first plurality of edges.*” *Id.*; Ex. 2003 [Malek Decl.] ¶ 44. Petitioner therefore must show that Brezinski teaches identifying relationships between pairs of entities—not merely recording events involving pairs of entities.

Petitioner does not make that showing. Its theory depends on treating Brezinski’s *events* as the claimed *relationships*. For the claimed “first plurality of edges,” Petitioner relies on Brezinski’s disclosure that its edges correspond to past events between entities, asserting without explanation that a “specific event/interaction” *is* a “relationship.” Pet., 28 (“[E]ach edge represents a *specific event/interaction—i.e., a relationship—*between the pair of entities[.]”). For the separately recited “first relationship,” which the claims require identifying from

received streaming data, Petitioner again relies on the same past events, arguing that Brezinski identifies the claimed relationship because it adds edges corresponding to “recently detected events.” *Id.*, 34. Thus, for both relationship limitations, Petitioner relies upon Brezinski’s events being relationships.

But the Petition does not—and cannot—justify that incorrect equivalence. In the ’628 patent, “events” and “relationships” are different claim terms. Data about events is received, while relationships are identified based on that data. *See* Section III.A.1. Petitioner ignores that distinction and fails to demonstrate that Brezinski’s event records constitute the claimed “relationships” between entities. *See* Section III.A.2.

1. The ’628 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 ... portion of the streaming data [about events] identify a first *relationship* between a pair of entities

Ex. 1001 [’628] cls. 1; *see also*, cl. 11 (reciting “streaming data comprising time-stamped data about *events*,” and “identify[ing] a first *relationship* between a pair of entities,” and later reciting “for a first *event* associated with a node”).

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 generating a graph edge representing the associated event. 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.] ¶ 47.

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 ’628’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 ’628 patent explains that in its graph, a relationship forming an edge between nodes that represent entities may be qualified by a “label”; for example, an edge indicating that two people know each other may be labeled “knows.” Ex. 1001 [’628] 7:51–61. Thus, the patent describes graph edges as relationships between entities, 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 [’628] 28:8–11. The ’628 specification illustrates several examples of these relationships in, for instance, Figure 22:

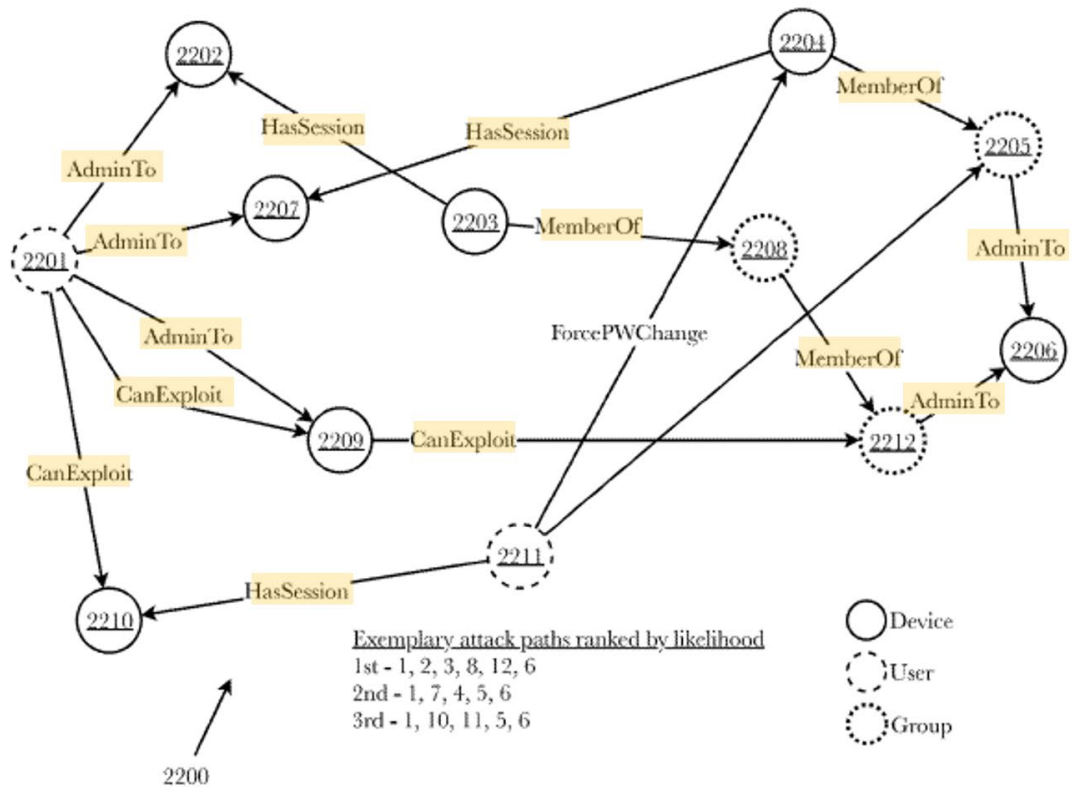


Fig. 22

Id., Fig. 22 (annotated); *id.*, 28:42–45 (“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 can correlate 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 [’628] 24:8–16. Similarly, the specification explains that the system can “maintain an up-to-date model of the network in real-time.” *Id.*, 26:4–8. 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.] ¶¶ 49–51.

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 [’628] 24:63–64. 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 ’628 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.] ¶ 52.

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

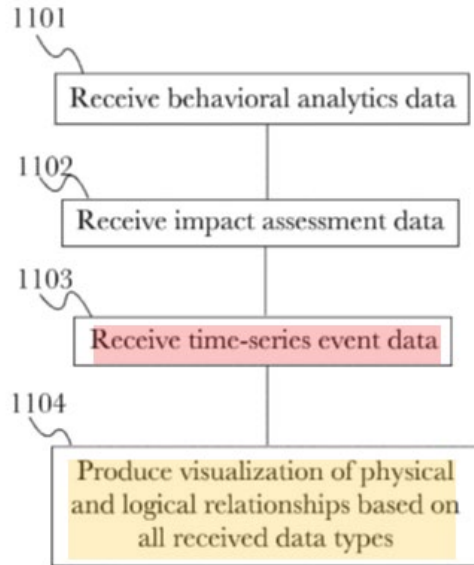


Fig. 11

1100

Ex. 1001 [’628] Fig. 11 (annotated). 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., 24:8–16.

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.*, 24:5–8. Thus, event data is received and incorporated, while the resulting graph visualization represents physical and logical relationships. *See also id.*, 23:40–57 (in Figure 10, state observation “information may be received continuously, passively collecting events and monitoring activity over time while feeding 1002 collected information into a graphing service 145 for use in producing time-series graphs 1003 of states and changes over time.”); *see also id.*, 27:59–28:4 (“time-series information (as described previously, referring to FIG. 10) may be received and incorporated, updating CPG information as changes occur and events are logged. This information may then be used ... to produce a meaningful and contextualized visualization of a security infrastructure that reflects the current state of the internal relationships present in the infrastructure.”). Event data may be an input from which relationship information is derived or updated, but events and relationships are not the same thing. Ex. 2003 [Malek Decl.] ¶ 53.

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 ’628 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 [’628] 28:42–45, Fig. 22.

Ex. 2003 [Malek Decl.] ¶ 55. And this accords with common usage. We may infer from events—a woman dons an elegant white dress with a veil, a religious figure pronounces vows, the two kiss—that a couple is in a married relationship.

Accordingly, the claim language, specification, and ordinary meanings all confirm that “event” and “relationship” are distinct. 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 inserting the words “*i.e.*, a relationship.” Petitioner still had to identify the relationship allegedly taught by Brezinski and explain why Brezinski’s event record satisfies the relationship limitations. As explained below, neither the Petition nor Dr. Black makes this showing.

2. Petitioner Fails To Prove That Brezinski’s Events Are The Claimed Relationships.

Petitioner’s analyses of both relationship limitations rest on the same

unsupported equivalence: that a Brezinski event is the claimed relationship. For the first relationship limitation, Petitioner acknowledges that Brezinski's edges correspond to particular events, but then concludes that each edge represents a *“specific event/interaction—i.e., a relationship.”* Pet., 26–28. For the second relationship limitation, Petitioner again relies on Brezinski's events, arguing that the limitation is met because Brezinski uses “additional event data” to add edges “corresponding to recently detected events.” *Id.*, 34. Petitioner later expressly refers to the alleged “new relationship/event,” confirming that its theory treats the two concepts as interchangeable. *Id.*, 37.

Petitioner's assertions that Brezinski's event edges represent relationships do not establish either claimed requirement. The first relationship limitation 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 [’628] cls. 1, 11. The second relationship limitation separately requires identifying “a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges.” *Id.* Thus, Petitioner had to establish both that Brezinski's mapped edges correspond to relationships between entity pairs and that Brezinski identifies a relationship that does not correspond to any edge in the claimed first plurality of edges. Showing that Brezinski records an event involving two entities—and adds another edge for

another event—does not establish either relationship limitation.

The Petition’s failure is not merely a matter of terminology. As explained below, the evidentiary record exposes the missing relationship in four related respects. First, neither the Petition nor Dr. Black provides technical reasoning supporting the asserted equivalence between Brezinski’s events and the claimed relationships; Dr. Black substantially repeats the Petition’s conclusion without adding independent technical analysis. *See* Section III.A.2(a).

Second, Brezinski’s actual disclosures characterize its individual edges as records of particular time-stamped events, and the event types cited by Petitioner do not themselves identify the relationship Petitioner contends is represented. Petitioner relies upon Brezinski’s Figure 4 but it only confirms that its mapped edges encode event records, in contrast to the relationship indicators illustrated in the ’628 patent’s Figure 22. *See* Section III.A.2(b).

Third, Petitioner’s “new relationship” theory fails for an additional reason. Even if one were to assume, *arguendo*, that a Brezinski event is a relationship, the claims require identifying a relationship that “***does not correspond*** to any of the first plurality of edges.” Ex. 1001 [’628] cls. 1, 11. Petitioner argues that Brezinski satisfies that requirement because Brezinski can add “additional edges 404 ***corresponding*** to recently detected events.” Pet., 34. But that disclosure proves, at most, that Brezinski adds a new edge ***corresponding*** to an event. It does

not prove that the alleged relationship does ***not*** correspond to edge in the first plurality. *See* Section III.A.2(c).

Finally, neither Brezinski’s generic description of graph theory nor Petitioner’s proposed combination with Crabtree supplies the missing limitation. *See* Section III.A.2(d).

These deficiencies confirm that Petitioner has identified events and event records, but has not demonstrated the “***relationships***” required by the claims.

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

Petitioner’s theory depends on an unstated and unsupported premise. Although the claims separately recite data “about events” and “relationship[s]” identified from that data, Petitioner treats those terms as interchangeable for purposes of its Brezinski mapping. Petitioner provides no basis for that equivalence in the claim language, the specification, the prosecution history, or the extrinsic record.

And 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 III.A.1. Petitioner, however, never acknowledges or addresses that distinction. *See* Pet., 26–28, 34. It never identifies the relationship allegedly taught by a Brezinski event, explains why the event

occurrence itself constitutes that relationship, or identifies what makes one alleged relationship different from another. Instead, Petitioner repeatedly substitutes “relationship” for Brezinski’s “event” and proceeds, without explanation, as though the limitation has been met.

Indeed, Petitioner continues to conflate “relationship” and “event” throughout its Petition without any explanation. For the relationship limitations, Petitioner treats Brezinski’s event edges as relationships, asserting that “each edge represents a specific event/interaction—i.e., a relationship.” Pet., 28. But for later limitations reciting “event[s],” Petitioner relies on the same type of Brezinski edges as events. For example, Petitioner argues that “because edges represent events,” Brezinski’s edges “indicate an anomalous event associated with a node in the graph.” *Id.*, 40. And Petitioner argues that a node corresponds to a “respective event” because of “an edge connecting” that node to the node associated with the anomalous event. *Id.*, 45. Petitioner thus uses Brezinski’s edges as “relationships” when the claim requires relationships and as “events” when the claim requires events, without articulating any principled distinction between the two.

Petitioner’s unsupported assertions cannot satisfy Petitioner’s burden. *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)) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated

reasoning with some rational underpinning to support the legal conclusion of obviousness.”); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”).

Petitioner cites its expert, Dr. Black, but he does not fill the gap. His declaration is equally conclusory and substantially repeats the Petition. *Compare* Pet., 26–28 *with* Ex. 1003 [Black Decl.] ¶¶ 76–77. Like the Petition, he too equates events with relationships and in exactly the same conclusory terms: “for each edge in Brezinski’s graph, the edge represents (i) *a specific event/interaction—i.e., a relationship ...*” *Id.*, ¶ 77. 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 III.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 explained 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 Brezinski passages establish that its individual edges record events. Dr. Black supplies no technical reasoning establishing that those events are the claimed relationships.

b. Brezinski’s Individual Event Records Do Not Establish The Claimed Relationships.

Petitioner’s mapping turns on what Brezinski’s individual edges represent. For the first relationship limitation, Petitioner relies on Brezinski’s individual edges 404(1) as the claimed graph edges and argues that each edge’s “specific event/interaction” is the claimed relationship. Pet., 26–28. For the second relationship limitation, Petitioner again relies on Brezinski’s event edges, asserting that adding edges for “recently detected events” identifies the claimed first

relationship. *Id.*, 34. Thus, Petitioner can satisfy the relationship limitations only if Brezinski's individual event edges disclose the claimed relationships.

But Brezinski repeatedly characterizes those edges as records of particular events. As Dr. Malek explains:

Brezinski teaches that its event data comprises individual event descriptions. Each event description identifies the initiating entity, the target entity, a timestamp, an event type, a user identifier, and potentially other event attributes. Ex. 1004 [Brezinski] 5:65–6:10, 6:37–44, Figs. 2–3. Figure 3, for example, depicts individual event records having event types such as “ssh,” “remotecall,” “launchprocess,” and “dataaccess,” each accompanied by a particular timestamp. *Id.*, Fig. 3.

Brezinski then describes Figure 4 as a graph comprising “an arrangement of events” and explains that individual edges 404(1) “each correspond to a particular event.” *Id.*, 8:29–40. Each individual edge may include the timestamp, event type, and user identifier of its associated event. *Id.*, 8:63–9:3. Brezinski's claim 1 likewise recites edges “indicating an event” by connecting vertices corresponding to the entities included in the event. *Id.*, cl. 1.

Thus, Brezinski's individual edges record particular time-stamped occurrences. They identify who initiated an event, the event's target, the type of event, the user involved, and when the event occurred. Standing alone, those event records do not identify the claimed relationship Petitioner contends is represented by the edge.

Ex. 2003 [Malek Decl.] ¶¶ 59–61.

Nor do the particular event types on which Petitioner relies supply the claimed relationships. Petitioner identifies “‘a network connection,’ ‘a communication over a network,’ ‘a login,’ or an ‘access to a resource’ or ‘access ... to a process.’” Pet., 26. But Brezinski identifies each of those items as a type of event recorded in an event description. Ex. 1004 [Brezinski] 6:37–7:32. In Brezinski, the event type identifies what occurred at a particular moment in time; it does not identify what relationship exists between the entities. Ex. 2003 [Malek Decl.] ¶ 62.

The examples make the deficiency concrete, demonstrating that the distinction is not merely semantic. As Dr. Malek explains:

For example, consider Brezinski’s exemplary 4-event graph consisting of four network SSH connection events. *See* Ex. 1004 [Brezinski] 10:4–33. Three of those events are SSH connections from “host1” to “host2” by the user “root.” Brezinski’s system dutifully records each connection *event* along with an associated timestamp (*id.*), but it is impossible to tell from that exemplary graph 118 whether, either at any given point or at present, the user “root” actually had or has an active SSH session (or how many of them). For example, an SSH connection can be terminated at any point after its original connection event for any number of reasons, such as a willful disconnection by the user, a network interruption, a loss of power to host2, *etc.* Similarly, Brezinski treats a network connection as an event

occurring at a particular time. *Id.*, 6:37–49. In a system taught by the ’628 patent, an actual connection might be captured by the presence of an edge corresponding to the specification’s exemplary “HasSession” relationship between host1 and host2, which would be updated upon receipt of streaming data about events that might cause a *dis*connection. The login occurrence—a discrete event in time—and the resulting relationship are not the same information.

Ex. 2003 [Malek Decl.] ¶ 63.

Similarly, an access to a resource or process records that an access occurred. The event does not itself identify whether the access resulted from an administrative relationship, group membership, an existing session, an exploitation capability, or some other relationship between the entities. A communication over a network likewise records that a communication occurred, but does not identify the physical or logical relationship under which the communication occurred. Ex. 2003 [Malek Decl.] ¶ 64. Petitioner never identifies which relationship it contends is represented by any of these events or explains why the occurrence itself is that relationship.

Petitioner and Dr. Black also rely upon Brezinski’s Figure 4. But that figure does not cure the deficiency; it confirms it. Brezinski describes Figure 4 as an arrangement of event data, including individual edges 404(1) that “each correspond to a particular event.” Ex. 1004 [Brezinski] 8:29–40. Its callout expressly

identifies edge 404(1) as “indicating event(s) initiated by the first entity and targeting the second entity,” and the edge contains a “timestamp attribute,” “event type attribute,” “user attribute,” and “risk metric.” *Id.*, Fig. 4; *see also id.*, 8:29–9:3. The multiple parallel edges between certain vertex pairs represent multiple event occurrences involving the same entities. *Id.*, 8:43–52. That is materially different from the ’628 patent’s Figure 22, which expressly identifies relationship information:

Petitioner’s Reliance Upon Brezinski’s Figure 4’s Event Data Only Confirms The Absence Of Identified Relationships Between Entities							
Brezinski’s Figure 4 Encodes Particular Event Records: The diagram shows a graph with vertices 402(1) through 402(9). Vertex 402(1) is associated with the first entity, and vertex 402(2) is associated with the second entity. The table below shows the event data for edge 404(1): <table border="1"> <thead> <tr> <th colspan="2">Edge(s) 404(1) (E.G., INDICATING EVENT(S) INITIATED BY THE FIRST ENTITY AND TARGETING THE SECOND ENTITY)</th> </tr> </thead> <tbody> <tr> <td>TIMESTAMP ATTRIBUTE 406</td> <td>USER ATTRIBUTE 410</td> </tr> <tr> <td>EVENT TYPE ATTRIBUTE 408</td> <td>RISK METRIC 412</td> </tr> </tbody> </table> FIG. 4 Ex. 1004 [Brezinski] Fig. 4	Edge(s) 404(1) (E.G., INDICATING EVENT(S) INITIATED BY THE FIRST ENTITY AND TARGETING THE SECOND ENTITY)		TIMESTAMP ATTRIBUTE 406	USER ATTRIBUTE 410	EVENT TYPE ATTRIBUTE 408	RISK METRIC 412	The ’628’s Figure 22 Expressly Identifies Relationship Information: The diagram shows a graph with vertices 2201 through 2214. The graph illustrates relationship information between entities. The relationships are as follows: 2201 (Device) - AdminTo -> 2202 (Device) 2201 (Device) - AdminTo -> 2207 (Device) 2201 (Device) - AdminTo -> 2209 (Device) 2201 (Device) - CanExploit -> 2210 (Device) 2202 (Device) - HasSession -> 2203 (Device) 2203 (Device) - MemberOf -> 2204 (Device) 2204 (Device) - MemberOf -> 2205 (User) 2205 (User) - AdminTo -> 2206 (Device) 2206 (Device) - AdminTo -> 2212 (Device) 2207 (Device) - HasSession -> 2208 (Device) 2208 (Device) - ForcePWChange -> 2211 (Device) 2209 (Device) - CanExploit -> 2211 (Device) 2210 (Device) - HasSession -> 2211 (Device) 2211 (Device) - MemberOf -> 2214 (Device) Exemplary attack paths ranked by likelihood 1st - 1, 2, 3, 8, 12, 6 2nd - 1, 7, 4, 5, 6 3rd - 1, 10, 11, 5, 6 Legend: ○ Device ○ User ○ Group Ex. 1001 [’628] Fig. 22
Edge(s) 404(1) (E.G., INDICATING EVENT(S) INITIATED BY THE FIRST ENTITY AND TARGETING THE SECOND ENTITY)							
TIMESTAMP ATTRIBUTE 406	USER ATTRIBUTE 410						
EVENT TYPE ATTRIBUTE 408	RISK METRIC 412						

As shown above, Figure 22's edges are expressly labeled with "relationship indicator[s]" such as "AdminTo," "MemberOf," "HasSession," "CanExploit," and "ForcePWChange." Ex. 1001 ['628] Fig. 22; *see also id.*, 28:42–45. 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, Brezinski's Figure 4 identifies what event occurred, when it occurred, and which entities participated in it. The point is not that the claims require the specific labels used in Figure 22. The point is that Figure 22 illustrates relationships, while Figure 4 depicts events. Ex. 2003 [Malek Decl.] ¶ 65. Petitioner itself elsewhere characterizes Brezinski's graph the same way, referring to the traversed graph as an "event graph" and relying on its edges as events for the later "event" limitations. Pet., 46–47.

Thus, Brezinski's individual edges do what Brezinski says they do: record particular event occurrences using event-record attributes. They do not record relationships. Accordingly, Brezinski's event-edge disclosures and Figure 4 do not establish the claimed relationships.

c. Even Assuming Brezinski's Events Were Relationships, Petitioner Fails To Show A Relationship That "Does Not Correspond To Any" First-Plurality Edge.

Even if we were to assume, incorrectly, that events are relationships, Petitioner's theory still fails as to the requirement to identify "a first relationship

between a pair of entities of the first plurality of entities *that does not correspond* to any of the first plurality of edges.” Ex. 1001 [’628] cls. 1, 11.

Petitioner relies on Brezinski’s disclosure that, upon receiving “additional event data,” its graph may incorporate “additional edges 404 corresponding to recently detected events.” Pet., 34. From that disclosure, Petitioner reasons that the “‘additional edges’ are by their name not pre-existing edges,” and that identifying a new event therefore identifies the claimed relationship that does not correspond to any first-plurality edge. *Id.*; Ex. 1003 [Black Decl.] ¶ 88.

That reasoning does not follow. The claims do not merely require adding an edge that was not previously in the graph. They separately require identifying “a first relationship ... *that does not correspond* to any of the first plurality of edges” and then adding “a first edge corresponding to the first relationship,” where “the first edge is not of the first plurality of edges.” Ex. 1001 [’628] cls. 1, 11. Thus, even if Brezinski’s “additional edge” is new, Petitioner still had to show that the alleged relationship corresponding to that edge did not already correspond to any edge in the first plurality. Petitioner never makes that showing.

Petitioner relies on Brezinski’s disclosure that, after receiving “additional event data,” the graph may incorporate “*additional edges 404 corresponding to recently detected events*,” and asserts that those “‘additional edges’ are by their name not pre-existing edges.” Pet., 34; Ex. 1003 [Black Decl.] ¶ 88. But that

argument proves the wrong thing. Brezinski's cited disclosure says that the added edges *do* "correspond[] to" the recently detected events. *Id.* Thus, on Petitioner's own premise that those events are the claimed relationships, Brezinski teaches only that the alleged relationships correspond to prior edges. It does not teach that the alleged relationship "does not correspond to any of the first plurality of edges."

Petitioner attempts to bridge that gap by asserting that the "additional edges" are "not pre-existing edges." Pet., 34. But the claim distinguishes between two different requirements: first, identifying a relationship that "does not correspond to any of the first plurality of edges"; and second, adding a new edge corresponding to that relationship, where the new edge "is not of the first plurality of edges." Ex. 1001 ['628] cls. 1, 11. Petitioner's "not pre-existing edge" assertion addresses, at most, the second requirement. It says nothing about the first. A newly added edge may be new to the graph, but that does not establish that the underlying relationship did not already correspond to some edge in the first plurality.

Indeed, Petitioner's cited language cuts against its theory. Pet., 34 (citing Ex. 1004 [Brezinski] 17:23-26). The cited portion of Brezinski does not disclose identifying an event/relationship and determining that no existing edge corresponds to it. Nor does the cited portion disclose any comparison between a newly detected event and the existing first plurality of edges. The only correspondence Petitioner identifies falls short of what is required: "additional edges 404 *corresponding* to

recently detected events.” Ex. 1004 [Brezinski] 17:23-26. At most, Petitioner shows is a disclosure of correspondence between an event and an edge. But what Petitioner needed to show and did not is a disclosure of non-correspondence between a relationship and every edge in the first plurality.

Petitioner’s theory therefore depends on an unstated assumption: that because an edge is “additional,” the event or relationship represented by that edge necessarily “does not correspond to any” earlier edge. But Petitioner never explains why that follows. “Additional” modifies the edge; it does not establish anything about whether the alleged relationship already corresponded to an existing edge. Treating every newly added edge as automatically satisfying the separate “does not correspond” limitation collapses two distinct claim requirements into one and reads the “does not correspond” language out of the claims. That implicit and unsubstantiated construction is improper. *Becton*, 616 F.3d at 1257 (“Claims must be ‘interpreted with an eye towards giving effect to all terms in the claim.’”); *Innova/Pure Water, Inc. v. Safari Water Filtration Sys.*, 381 F.3d 1111, 1119 (Fed. Cir. 2004) (“[A]ll claim terms are presumed to have meaning in a claim.”).

Accordingly, even accepting Petitioner’s premise that Brezinski’s events are relationships, Petitioner establishes, at most, that Brezinski may receive additional event data and add another edge corresponding to a recently detected event. That

is not the claimed identification of a relationship that “does not correspond to any of the first plurality of edges.” Petitioner therefore fails to demonstrate this limitation of claims 1 and 11 for this additional reason.

d. Brezinski’s Generic Graph Definition Does Not Fill The Gap.

Petitioner also relies on Brezinski’s generic statement that “[a] graph is a representation of a plurality of objects and one or more relationships between one or more pairs of the objects.” Pet., 27. But that general statement does not establish what Brezinski’s edge 404(1) represents.

Brezinski defines edge 404(1) as corresponding to a “particular event,” and by explaining that multiple such edges between the same vertices indicate multiple events occurring at different times. Ex. 1004 [Brezinski] 8:37–52. Thus, Petitioner’s generic graph definition cannot convert Brezinski’s time-stamped event records into the claimed relationships between entities.

Brezinski’s specific disclosures confirm the point. Brezinski describes its generated graph as one that “interrelates or correlates a plurality of events.” Ex. 1004 [Brezinski] 2:31–32. It defines edge 404(1) as corresponding to a “particular event.” *Id.*, 8:37–40. It separately defines overlay edge 404(2) as summarizing events of a particular type. *Id.*, 8:40–42. And it repeatedly states that its individual edges indicate events, include timestamps identifying when those events occurred,

and are categorized by event type. *Id.*, 2:45–62, 6:37–64, 8:29–9:3; *id.*, cl. 1. A general statement that graphs may represent relationships therefore cannot override Brezinski’s clear statements about what edge 404(1) represents. Ex. 2003 [Malek Decl.] ¶ 74. Petitioner had to explain why Brezinski’s particular event occurrence, represented by the particular edge it maps, is the claimed relationship. It did not.

And if we were to assume, as Petitioner does, that all graph edges represent relationships—even when Brezinski makes expressly clear that its edges represent events—that would render the “relationship” limitations meaningless and further negate the distinction made between “relationships” and “events” in the claims.

See also Section III.A.1.

* * *

Accordingly, Petitioner fails to demonstrate that Brezinski’s particular event records are the claimed relationships, that Brezinski’s mapped first-graph edges correspond to respective relationships between entity pairs, or that adding an edge for a recently detected event identifies a relationship that “does not correspond to any of the first plurality of edges.” Petitioner therefore has not shown that Brezinski teaches the relationship limitations of claims 1 and 11.

B. Petitioner Fails To Demonstrate That Brezinski Teaches “Perform A First Correlation ... To Identify A First Plurality Of Correlated Nodes” (All Claims).

The claims require “for an anomalous event associated with a node in the modified representation of the first graph, *perform a first correlation* using the modified representation of the first graph to identify a first plurality of correlated nodes.” Ex. 1001 [’628] cl. 1; *see also id.*, cl. 11 (reciting corresponding limitation for “a first event associated with a node”). Petitioner argues that Brezinski teaches this limitation because “Brezinski teaches to ‘*traverse* a graph’ along edges and identify ‘the edges 404 and the vertices 402’ associated with a rarity and/or risk metric that satisfies a certain threshold.” Pet., 39. Petitioner separately relies on Brezinski’s disclosure concerning interactions with a designated suspicious entity, such as a honey pot, and characterizes the identification of graph elements connected to that entity as a correlation. *Id.*, 43–45. This “honey pot” is one of the metrics Brezinski can use to “travers[e]” its graph and is thus part of Brezinski’s traversal. *See* Ex. 1004 [Brezinski] 12:12–14 (“the subset of the graph 118 determined by traversing the graph 118 may be described in anomalous activity data 122”); *id.*, 12:35–53 (“one or more additional criteria” such as the “honey pot” “may be employed to determine whether the edges 404 or vertices 402 are to be included in the subset of the graph 118 designated as the anomalous activity data 122.”); Ex. 2003 [Malek Decl.] ¶ 78.

Thus, Petitioner relies on Brezinski's traversal and graph-element-selection disclosures as the claimed correlation. But Brezinski expressly discusses "correlation" elsewhere, when describing the generation of its graph, and Petitioner does not rely on those disclosures to satisfy this limitation. Petitioner fails to explain why Brezinski's separately described traversal or selection process is the claimed "first correlation."

As an initial matter, Petitioner's explanation of why Brezinski's traversal is correlation is conclusory. Petitioner states:

Brezinski teaches to "traverse a graph" along edges and identify "the edges 404 and the vertices 402" associated with a rarity and/or risk metric that satisfies a certain threshold (*perform a correlation ... to identify a first plurality of correlated nodes*)

and then asserts that Brezinski's "breadth-first graph traversal performs the claimed correlation because it uses the graph to correlate a plurality of nodes with anomalous network activity." Pet., 39 (emphasis in original).

That reasoning is conclusory and circular. The first statement describes Brezinski's traversal and threshold-based selection and with Petitioner's bare assertion that the "perform a correlation" limitation is met. The second asserts that the traversal performs correlation because it "correlate[s]" the nodes. Neither statement identifies what operation within Brezinski's traversal constitutes the

alleged correlation or explains why that operation satisfies the claimed “first correlation.” Petitioner discusses traversal, calls it correlation, and proceeds as though the limitation has been met.

The cited Brezinski disclosures do not fill the gap. Brezinski describes selecting a current vertex, selecting an edge originating from that vertex, determining whether the edge satisfies specified risk and rarity criteria, including qualifying edges and their connected vertices in anomalous activity data, and continuing through the graph. Ex. 1004 [Brezinski] 3:52–67, 17:39–18:44, Fig. 11. Those disclosures explain how the graph is searched, how edges are evaluated, and which graph elements are included in the resulting subset representing “anomalous activity data.” They do not explain why that search-and-selection process performs a correlation. Ex. 2003 [Malek Decl.] ¶ 81

Petitioner’s reliance on “breadth-first” traversal does not supply the missing correlation. Brezinski explains that a breadth-first traversal explores neighboring nodes before exploring nodes located deeper along a possible branch. *Id.*, 3:60–63. That describes the order in which the graph is searched. It does not explain why searching the graph in that order performs the claimed correlation, regardless of whether the search is “breadth-first” or “depth-first.” Ex. 2003 [Malek Decl.] ¶ 82.

Petitioner’s treatment of Figure 7 confirms the same deficiency. Brezinski describes Figure 7 as “anomalous activity data” comprising edges that satisfy

specified risk and rarity thresholds and vertices connected by those edges. Ex.

1004 [Brezinski] 11:44–12:14, Figs. 6–7. Petitioner reproduces Figure 7 and adds a red annotation identifying vertices 402(2), 402(4), and 402(5) as a “First Plurality of Correlated Nodes.” Pet., 42. But “First Plurality of Correlated Nodes” is Petitioner’s annotation, not Brezinski’s disclosure. Adding the claim terminology to Brezinski’s figure does not demonstrate that the traversal used to create the depicted anomalous-activity subset performs the claimed correlation. Ex. 2003 [Malek Decl.] ¶ 83.

Petitioner’s honey pot argument fares no better. Petitioner asserts that Brezinski teaches “designating an entity (such as a honey pot) as associated with anomalous behavior and correlating the node corresponding to that entity with any nodes connected to it.” Pet., 43. But the cited Brezinski passage does not describe correlation. It explains that an edge may be included in anomalous activity data if it connects to a vertex associated with a particular entity, and that “any interaction with the honey pot entity” may be flagged as potentially malicious and included in the anomalous activity data. Ex. 1004 [Brezinski] 12:35–53. Brezinski thus discloses an additional criterion for selecting graph elements for inclusion in anomalous activity data. Petitioner supplies the characterization that this selection “correlat[es]” the connected nodes, but does not explain why applying that selection criterion performs the claimed correlation. Ex. 2003 [Malek Decl.] ¶ 84.

Dr. Black merely repeats that traversal along edges satisfying risk or rarity thresholds “perform[s] a correlation,” and concludes that breadth-first traversal correlates nodes with anomalous network activity. Ex. 1003 [Black Decl.] ¶ 96. Dr. Black later explains that “Brezinski’s graph traversal therefore includes a first ‘correlation’ because it uses the structure of the graph—relationships captured by edges between vertices—to identify other graph elements related to the anomalous activity.” *Id.*, ¶ 99. But that merely restates the disputed conclusion: because the vertices are connected, Dr. Black calls them correlated. It does not explain why Brezinski’s traversal, threshold testing, or inclusion of connected vertices in anomalous activity data constitutes the claimed “first correlation.” His honey pot analysis similarly begins with a designated suspicious entity, identifies connected graph elements, and concludes that the resulting selection is a correlation. *Id.*, ¶¶ 100–102. Again, the conclusion supplies the word “correlation,” but no technical reasoning connecting Brezinski’s disclosed operation to that claim requirement.

As explained above, such conclusory assertions cannot satisfy Petitioner’s burden. *See* Section III.A.1; *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). And Dr. Black’s equally conclusory testimony cannot fill in the gaps. *See* Section III.A.1; 37 C.F.R. § 42.65(a); *Virtek Vision Int’l ULC v. Assembly Guidance Sys.*,

Inc., 97 F.4th 882, 887 n.2 (Fed. Cir. 2024); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, 15 (Aug. 24, 2022).

Petitioner’s failure to explain what “correlation” means is especially insufficient because Brezinski discloses correlation² and traversing a graph as separate and distinct concepts. As Dr. Malek explains:

Brezinski distinguishes between correlation and traversing the graph. Brezinski explains that its graph “correlates a plurality of events detected on host devices.” Ex. 1004 [Brezinski] 2:8–11. Indeed, Brezinski repeatedly describes using correlation (also referred to as “interrelation”) to generate the graph Petitioner alleges is the first graph (Pet., 20–22). *E.g.*, Ex. 1004 [Brezinski] 2:31–32 (“The collected event data may be analyzed to ***generate a graph that interrelates or correlates*** a plurality of events.”); *id.*, 8:23–27 (“The analysis device(s) 114 may execute a graph generation module 116 configured to access the event data 110 and generate one or more graphs 118 that ***graphically correlate*** or otherwise describe at least some of the events included in the event data 110.”). Brezinski then teaches that after the graph of correlated events is generated, that graph is used to “identify[] anomalous activity by ***traversing*** the graph according to one or both of

² This is not to suggest that Brezinski’s “correlation” satisfies the claims either. As explained later, it does not and Petitioner does not rely upon Brezinski’s correlation for good reason.

a rarity metric and a risk metric...” Ex. 1004 [Brezinski] 2:8–13; *see also id.*, 3:52–67 (“the graph may be traversed” after it is generated).

Notably, correlation/interrelation on the one hand and traversal on the other are a part of two distinct processes in Brezinski. Correlation/interrelation is shown in Figure 10 which “depicts a flow diagram of a process for generating a graph that *correlates* multiple events present in the event data.” Ex. 1004 [Brezinski] 1:54–60; *id.*, Fig. 10.

Traversal, on the other hand, is shown in Figure 11 which “depicts a flow diagram of a process for traversing or otherwise analyzing a graph to identify anomalous activity...” Ex. 1004 [Brezinski] 1:61–64. Indeed, the first step of Figure 11 involves “access[ing] a graph” that has already been created:

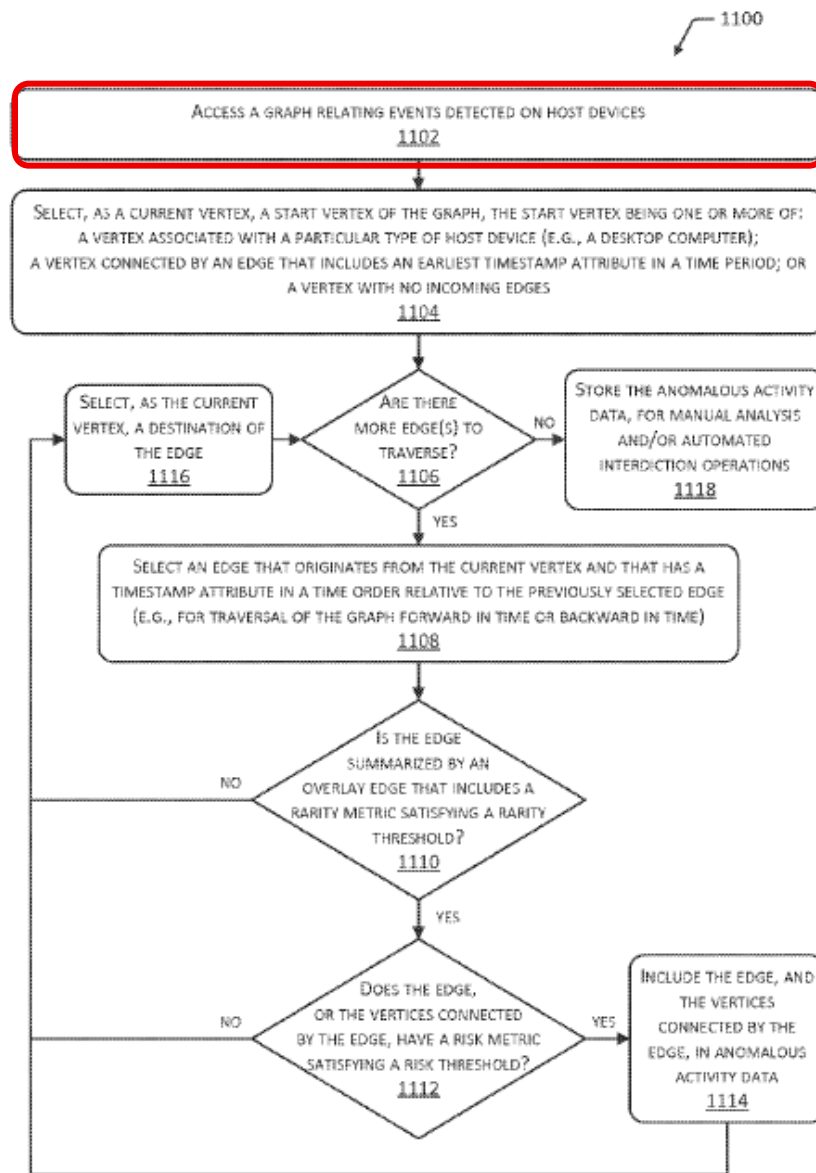


FIG. 11

Id., Fig. 11 (annotated).

Figure 11 and its corresponding discussion do not use the term “correlation” at all. *See* Ex. 1004 [Brezinski] Fig. 11, 1:61–64, 17:39–18:44. Instead, they describe traversing or analyzing an already-

generated graph to identify anomalous activity. The fact that Brezinski separately discloses graph generation through correlation and later graph traversal underscores that Petitioner was required to explain why the cited traversal disclosures nevertheless satisfy the claimed correlation limitation. Petitioner never provides that explanation.

Ex. 2003 [Malek Decl.] ¶¶ 86–89.

The Petition’s element-specific mapping confirms that it relies on Brezinski’s “traversal” process, *not* its “correlation” process. *See* Pet., 39–45. It relies on risk- and rarity-based traversal and, alternatively, the selection of graph elements associated with a known compromised or honey pot entity. *Id.* It does not rely on Brezinski’s express graph-generation correlation disclosures, acknowledge the distinction between the two operations, or explain why the later traversal or selection process nevertheless constitutes correlation.

And Petitioner does not (and cannot) rely on Brezinski’s actual correlation process for good reason. As Dr. Malek explains, Brezinski’s correlation is used to generate the graph rather than to identify nodes correlated to an event:

The claims require first generating a graph that is updated with new nodes and edges. Ex. 1001 [’628] cls. 1, 11. When there is an “event associated with a node,” the claims require using the generated and updated graph to perform a correlation and identify correlated nodes. *Id.* By contrast, Brezinski’s express correlation occurs earlier,

during graph generation itself, and correlates events (Brezinski's edges) rather than nodes.

As Brezinski makes clear, its correlation is used in the process of generating the graph that then later gets analyzed if there is an anomalous event. Brezinski teaches that “[e]vent data may be collected” which then “may be analyzed to *generate a graph* that interrelates or *correlates a plurality of events*.” Ex. 1004 [Brezinski] 2:14–15, 2:31–32. But the claims first require modifying a graph to include a new entity and new relationship before using that modified graph to perform a “first correlation” “for [an anomalous/a first] event” and “to identify a first plurality of correlated nodes.” Ex. 1001 [’628] cls. 1, 11.

In other words, the claims recite correlating nodes after the graph has been generated. Brezinski's express correlation disclosures concern the correlation of events, not the correlation of nodes after an event. Ex. 1004 [Brezinski] 2:31–32. Consequently, it is no surprise that Petitioner cannot rely on Brezinski's actual correlation process for the claimed “correlation.”

Ex. 2003 [Malek Decl.] ¶¶ 91–93.

Petitioner, thus, has identified disclosures concerning graph traversal. What Petitioner has not done is demonstrate that the cited *traversal* disclosures satisfy the claimed *correlation* limitations. Because the Petition relies on Brezinski's traversal rather than its actual correlation teachings—and never explains why

traversal and correlation are equivalent—Petitioner fails to demonstrate that Brezinski teaches “perform[ing] a first correlation ... to identify a first plurality of correlated nodes.”

IV. 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* pending
Colette Woo, *pro hac vice* pending
LOWENSTEIN & WEATHERWAX LLP

Date: July 8, 2026

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner Preliminary Response (the “POPR”) consists of 8,473 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 /

Date: July 8, 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	andrew.mason@klarquist.com
Cameron D. Clawson	cameron.clawson@klarquist.com
Caitlin C. Potter	caitlin.potter@klarquist.com
Frank Morton-Park	frank.morton-park@klarquist.com
Todd M. Siegel	todd.siegel@klarquist.com
Samuel B. Thacker	samuel.thacker@klarquist.com
	Msft-Qomplx@klarquist.com

Respectfully submitted,

/ Michael Cosley /

Date: July 8, 2026