

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE INC.,
Patent Owner.

Case IPR2023-00656
Patent 10,713,366

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE ‘366 PATENT DISCLOSES AND CLAIMS THREAT MODELING METHODS AND SYSTEMS NOT DISCLOSED OR SUGGESTED BY THE ASSERTED ART	5
A.	The ‘366 Patent Claims one or more Databases Storing Threats and Associations with Components	5
B.	The ‘366 Patent Also Discloses and Claims one or more Mapping Files Correlating the Threat Model Components with Visual Diagram Components of a Third Party Software Application	8
III.	THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION.....	11
IV.	PETITIONER’S CHALLENGES FAIL ON THE MERITS	11
A.	Keenan’s Risk Values are Not “Threats” as Claimed.....	12
B.	Keenan Also Fails to Disclose any “Mapping Files” as Claimed.....	19
C.	Zheng Alone or in Combination with Secondary References Fails to Disclose any “Mapping Files” “Correlating the Threat Model Components with Visual Diagram Components of a Third Party Software Application”	21
D.	Grounds 3-5 Fail to Remedy the Above-Identified Failures of Grounds 1 and 2	25
V.	CONCLUSION.....	26

TABLE OF AUTHORITIES

Cases

<i>Verdegaal Bros., Inc. v. Union Oil Co. of Cal.</i> , 814 F.2d 628 (Fed. Cir. 1987)	13
--	----

Statutes

35 U.S.C. § 311(b)	22, 26
--------------------------	--------

Rules

37 C.F.R. § 42.107	1
37 C.F.R. § 42.120(a).....	1

Other References

Consolidated Trial Practice Guide	15, 22
---	--------

Pursuant to 37 C.F.R. § 42.107, Patent Owner ThreatModeler Software Inc. (“TMS” or “Patent Owner”) files this preliminary response to the Petition, setting forth reasons why the Petition for *inter partes* review (“IPR”) of claims 1-20 of U.S. Patent No. 10,713,366 (the “’366 Patent”), as requested by IriusRisk, Inc. (“Petitioner”), should be denied.¹

I. INTRODUCTION

The ’366 Patent is entitled, “Systems and Methods for Automated Threat Model Generation from Third Party Diagram Files.” “Threat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” ’366 Pat., 1:56-57. The ’366 Patent discloses a novel threatmodeling software system and process that can generate a threat model from an imported file, and generate a threat report displaying each threat that is associated with threat model components and/or relationships between threat model components. As examples, the ’366 Patent explains that “this could include modeling the possible threats to commuting to work safely, modeling the possible threats to preventing the spread of an infectious disease, or modeling the possible attacks on a computer network (cybersecurity).” ’366 Pat., 9:1-5. A “threat report” can identify “threats, the status of identified threats (threat status), and the source(s) of identified threats,

¹ By submitting this Preliminary Response, no waiver of any argument is intended by Patent Owner. Patent Owner will have a right to file a complete response to the Petition, should the Board institute *inter partes* review. 37 C.F.R. § 42.120(a).

among other things.” ’366 Pat., 9:6-9. Exemplary threats disclosed in the ’366 Patent include specific dangers or vulnerabilities such as “bluejacking” where a modeled system includes a Bluetooth port, and “freeway collision” where the modeled process is “commuting to work.” ’366 Pat., 9:55-10:7. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” ’366 Pat., 24:64-25:1.

While software “exists for converting a [system or process] diagram of one type to another type of diagram file,” the ’366 Patent notes that no solution exists for converting a third party software diagram into a threat model. ’366 Pat., 2:47-54. Consistent with this disclosure, the challenged claims are directed generally to a software-based threatmodeling system or method that “may be able to take any diagram, in any file format, and convert it into a threat model.” ’366 Pat., 43:9-11.

Petitioner asserts five grounds against these challenged claims.

In Ground 1, Petitioner contends that each of the challenged claims is anticipated by the Keenan² reference.

² Ex. 1004, U.S. Patent No. 11,200,228 (“Keenan”).

In Ground 2, Petitioner contends that claims 1-4, 7-11, and 15-18 are rendered obvious by the Zheng³ reference in view of the Baker⁴ reference and the Jones⁵ reference (Petitioner refers to Zheng, Baker, and Jones collectively as the “References of Ground 2”).

In Ground 3, Petitioner contends that claims 2, 9, and 17 are rendered obvious by the References of Ground 2 further in view of the Galliano⁶ reference.

In Ground 4, Petitioner contends that claims 5-6, 12-14, and 19-20 are rendered obvious by the References of Ground 2 further in view of Keenan.

In Ground 5, Petitioner contends that claims 2, 5-6, 9, 12-14, 17, and 19-20 are rendered obvious by the References of Ground 2 further in view of the Knowledge of a POSITA.

However, in each ground, the asserted references—whether considered alone or in Petitioner’s asserted combinations—fail to disclose or suggest every claimed feature. For example, in Ground 1, Petitioner identifies Keenan as an anticipatory reference. But Keenan fails to disclose or suggest any “threat” or any database storing threats, as claimed. Rather, Keenan assigns a risk value, which is

³ Ex. 1005, U.S. Patent No. 10,503,907 (“Zheng”).

⁴ Ex. 1006, U.S. Patent Application Publication No. 2014/0236665 (“Baker”).

⁵ Ex. 1007, U.S. Patent No. 9,602,529 (“Jones”).

⁶ Ex. 1008, U.S. Patent No. 10,681,068 (“Galliano”).

a number, without identifying or storing any threat as claimed. Further, Keenan fails to disclose storing any threats in a database, as storing a value corresponding to a degree of risk is not what is claimed by the '366 Patent. The Petition also fails to establish the disclosure of any “mapping files” in Keenan, where “the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter ‘third party diagram components’).” Petitioner argues that “a mapping file is required to form a map,” but this argument relies on inherency without the necessary unpinning. As such, Petitioner’s inherency-based theory necessarily fails.

The References of Ground 2 are equally deficient in their disclosures, and further suffer from hindsight-based combinations unsupported by a POSITA’s motivation as required. For example, Petitioner fails to establish the disclosure or suggestion of the claimed “one or more mapping files” in any of the References of Ground 2, whether they are considered alone or in combination. In order to reach the claimed “mapping files” correlations recited in claim 1, Petitioner first invents a mapping file to capture the threat actor/threat target association of Zheng, and then invents a modification to repurpose the associations for use with Baker. But Baker has no need for a mapping file, as Baker behaves similarly to Keenan, without any express or suggested mapping files. Moreover, Petitioner’s motivation

for its proposed creations and combinations in order to recreate the challenged claims is limited to impermissible hindsight. Like Ground 1, Ground 2 also fails.

Finally, Grounds 3-5 are directed to dependent claims only, and the references relied upon in Grounds 3-5 are not added to cure any of the above-identified shortcomings of Grounds 1 and 2 against the challenged independent claims. The shortcomings identified for Grounds 1 and 2 also render Grounds 3-5 insufficient to establish unpatentability of any claim. As such, each challenge fails, and the Petition should be denied without institution.

II. THE ‘366 PATENT DISCLOSES AND CLAIMS THREAT MODELING METHODS AND SYSTEMS NOT DISCLOSED OR SUGGESTED BY THE ASSERTED ART

A. The ‘366 Patent Claims one or more Databases Storing Threats and Associations with Components

The exemplary threat modeling system disclosed in the ‘366 Patent includes one or more databases storing threats, threat model components, and associations there between.

Describing Figure 2, the ‘366 Patent describes a “representative example of a threat modeling process” which includes “generating a threat model ... for any application, process, or system under consideration.” ‘366 Pat., 8:65-9:1. The ‘366 Patent continues, “By non-limiting example, this could include modeling the possible threats to commuting to work safely, modeling the possible threats to preventing the spread of an infectious disease, or modeling the possible attacks on

a computer network (cybersecurity).” ’366 Pat., 9:1-5. A “threat report” can include “identified threats, the status of identified threats (threat status), and the source(s) of identified threats, among other things.” ’366 Pat., 9:6-9. As already introduced above, exemplary threats disclosed in the ’366 Patent include “bluejacking” where a modeled system includes a Bluetooth port, and “freeway collision” where the modeled process is “commuting to work.” ’366 Pat., 9:55-10:7. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” ’366 Pat., 24:64-25:1.

The data store 206 of the ’366 Patent stores “a plurality of threats 202 and threat model components ... 204,” and “each component and/or threat” may include “titles, definitions or descriptions, and/or associated images in the database 108.” ’366 Pat., 9:10-16. The “database allows for the correlation of any threat to any number of components and likewise, the correlation of any component to any number of threats.” ’366 Pat., 10:8-12. “[E]ach asset could have any number of threats that could threaten to compromise it. ... Some assets may be threatened by only a single threat, some may be threatened by two or three threats, or more, and so forth.” ’366 Pat., 24:26-32.

Similar to the described embodiments above, the challenged claims of the ’366 Patent recite a “database,” and in claim 1, the database comprises, in relevant

part, “a plurality of threat model components stored therein; and a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases.” Independent claims 8 and 16 include substantially similar features. As claimed, the “database” does not simply store a numeric value as a property or characteristic of a component. Rather, as claimed, the one or more databases expressly stores “a plurality of threats,” and associates each of the threats with “at least one of the threat model components through the one or more databases.”

Further, the '366 Patent expressly distinguishes between “threats” and the concept of “risk.” “[A]n interface of the system may list the most vulnerable components in ascending/descending order, along with the risk level for each listed component, the number of total threats to that component, and the number of open or unmitigated threats for that component.” '366 Pat., 25:8-12. As discussed, a “threat” may be associated with a risk level as disclosed in Figure 8 and the specification, but a risk level is different from a threat. Describing FIG. 8, the '366 Patent discloses, “The title ‘threats’ is shown near the top of a list of threats which are organized into rows and columns showing each threat's name, risk level, and attached labels.” '366 Pat., 14:5-9. Exemplary risk levels are relative values, *i.e.*, very high, high, or medium, but risk levels do not disclose threats to the system's components. '366 Pat., FIG. 8; 25:20-26.

B. The '366 Patent Also Discloses and Claims one or more Mapping Files Correlating the Threat Model Components with Visual Diagram Components of a Third Party Software Application

As discussed in the '366 Patent and introduced above, the disclosed “[t]hreat modeling systems” can include databases storing “threat model components and threats associated with one another.” '366 Pat., Abst. Additionally, “[o]ne or more mapping files coupled with the database(s) correlate the threat model components with visual diagram components of a third party software application.” *Id.* Additional disclosure related to the use of the mapping file in the importation of a third party diagram file is provided in FIG. 30, reproduced below, and the corresponding specification.

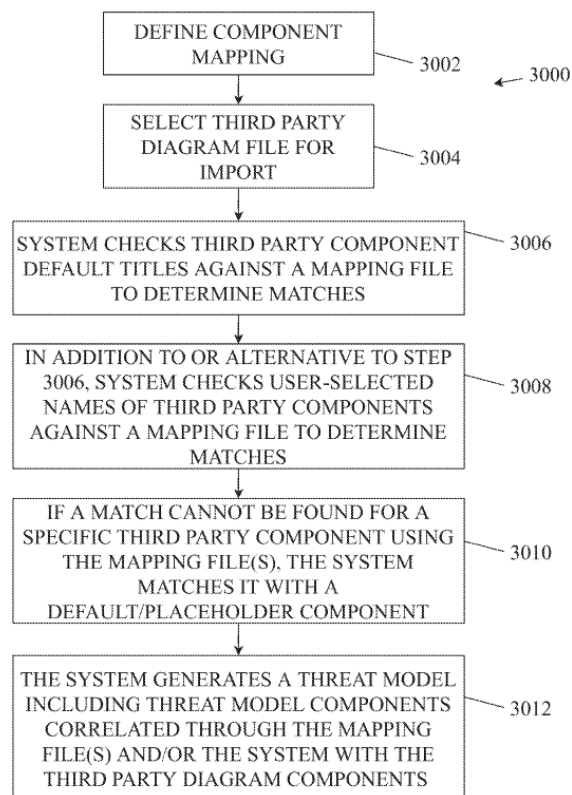


FIG. 30

As disclosed and described in FIG. 30, “FIG. 30 ... representatively illustrates step 3004 of selecting a file for import,” which the specification describes in more detail “with respect to the import interface 2500 of FIGS. 25-27.” ’366 Pat., 37:46-49. “The steps of checking components of the imported third party file against the mapping files is representatively illustrated by steps 3006 and 3008 of flowchart 3000 in FIG. 30.” ’366 Pat., 38:13-16. Where a mapping file does not include a match for a component to be imported from the third party software application, step 3010 can include “using a placeholder component” as shown in FIG. 30. ’366 Pat., 38:17-32.

Step 3012 includes generating a threat model. “Generating the threat model may include using the system to determine threats, threat sources, threat risk levels, threat statuses, security requirements, compensating controls, threat mitigations, and so forth—associated with the system/method or the like that was diagrammed in the third party software and imported to generate the threat model—and displaying these to the end user.” ’366 Pat., 39:47-54. As described and illustrated, steps 3006, 3008, 3010, and 3012 of FIG. 30 each involve the use of a mapping file.

The ’366 Patent describes exemplary mapping files. For example, as shown in FIGs. 28 and 29, “interfaces 2800 and 2900 show comma separated value (CSV) files (mapping files) that may be used by the system to correlate the third party

diagram components with threat model components previously stored in the one or more databases.” ’366 Pat., 37:14-18. In FIG. 28, the CSV mapping file “includes a table listing, for each listed item, a name given by an administrator, a value (which is the default title assigned to a component in the third party diagramming software), a comment (if any), and a global unique identifier (GUID) which is associated with a specific threat model component through the one or more databases. In this way any component of the third party diagramming software may be mapped to (correlated with) a corresponding threat model component stored in the one or more databases.” ’366 Pat., 37:18-24. For example, where a file to be imported includes an INTERNET GATEWAY, “the INTERNET GATEWAY threat model component would have previously been configured to match the details/properties of the INTERNET GATEWAY third party diagram component” through step 3002 component mapping. ’366 Pat., 28-45.

The ’366 Patent discloses other exemplary embodiments for the mapping file. *See, e.g., id.*, 37:50-59 (describing variations for populating CSV column characteristics). Additionally, the ’366 Patent discloses that other file formats than CSV could be used for a mapping file. “In implementations one or more tables in the database(s) could include the same information and could be used for mapping.” ’366 Pat., 38:33-36. However, where “one or more tables of the database are used for the mapping file(s), each table is, for the purposes of this

disclosure, a ‘file.’” ’366 Pat., 38:40-42. “In the implementation in which separate files, not in the database(s) are used, [the mapping files] could be stored on the one or more computing devices that comprise the system 100 (including user computers, servers, and so forth).” ’366 Pat., 38:36-40.

III. THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION

The Petitioner identifies four terms as requiring constructions: “third party software application,” “third party diagram components,” “visual representations of the threat model components,” and “threat model components.” Pet., 13-14. Without expressly agreeing to Petitioner’s proposed constructions, and without waiving its right to submit competing constructions in a Patent Owner Response, Patent Owner submits that the Board need not engage in any pre-institution claim construction of these terms. For the reasons presented in Section III below, Petitioner’s grounds each include fundamental flaws and fail to establish the disclosure of every claimed element in each independent claim. These findings do not require the Board to conduct any construction of the above-identified terms.

IV. PETITIONER’S CHALLENGES FAIL ON THE MERITS

Each challenge is facially deficient in establishing the unpatentability of any challenged claim. In Ground 1, Petitioner contends that Keenen anticipates claims 1-20, but this is wrong. Keenen fails to disclose any “threat” as claimed, including a “threat modeling method,” a “plurality of threat model components” and a

“plurality of threats,” and “a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.” Keenan’s disclosure of a risk value fails to identify any threat, and simply is a numeric value or color representing a degree of risk. There is no information associated with this value that identifies any threat to a component. Further, Keenan does not store any threat in a database.

Additionally, Petitioner’s anticipation-based challenge against claims 1-20 is faulty as Petitioner acknowledges that Keenan does not disclose a mapping file. Petitioner relies on its expert declaration to allege that Keenan’s disclosure of a “map” requires a mapping file, but Petitioner fails to establish that “one or more mapping files” is inherent or necessarily present in Keenan.

Ground 2 also fails. Petitioner points to Zheng’s mapping for the claimed “mapping file,” but then modifies Zheng in a manner unsupported by any evidence. In essence, Petitioner combines Zheng and Baker, and then further modifies that combination, thereby inventing Patent Owner’s invention. This obviousness-based challenge is guided by hindsight, not by proper motivation under the laws of obviousness.

A. Keenan’s Risk Values are Not “Threats” as Claimed

Claim 1’s preamble recites a “threat modeling method,” and the claimed steps include many features using the term, “threat.” For example, claim 1 also

recites, in relevant part, storing a “plurality of threat model components” and a “plurality of threats,” and “generating ... a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.” Independent claims 8 and 16 include substantially similar features. Keenan fails to disclose such features, and therefore cannot anticipate any challenged claim. “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

The ’366 Patent discloses very early in the specification that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” ’366 Pat., 1:56-57. “Threat modeling allows a user to analyze potential attack vectors and prioritize vulnerabilities.” ’366 Pat., 1:60-62. Keenan includes none of these features. In particular, Keenan does not identify threats or store threats, and does not detail or prioritize vulnerabilities. This fact is clear from Keenan’s disclosure about what a “risk” really means as used by Keenan, and what it is used for.

Initially, Keenan’s applicant is not a software company, a cybersecurity company, or an entity concerned with modeling “threats” for the purpose of analyzing potential attack vectors and detailing and/or prioritizing vulnerabilities.

Rather, Keenan was filed by and assigned to an insurance company: American International Group, Inc. Keenan assigns a risk value to certain aspects of a system, but the threats underlying that risk value are neither determined by Keenan nor important to Keenan. The purpose of Keenan is to provide a view that allows a user to see an overall risk associated with an infrastructure for business and insurance purposes, not to detail or prioritize vulnerabilities or threats. Keenan makes this clear in the specification:

Design of object classifications is suited to capture the properties of the information assets in a way that associates the risk, cost, quality, accountability of the assets to the product chain that produces calc[ulation]s which the business utilizes *to set premiums and reserves, manage investment risk and produce financial reports and compliance reports.*

Keenan, 1:33-38 (emphasis added).

Petitioner relies on Keenan’s disclosure of “risk” as satisfying the claimed “threat” features of the ’366 Patent. Specifically, Petitioner contends that a “POSITA would understand that Keenan’s ‘risk’ includes threats because measuring risk includes a determination of threats.” Pet., 23 (citing Keenan, 16:40-51, Ex. 1003, ¶79). However, this is improper under a theory of anticipation. A “petitioner asserting anticipation cannot rely on its expert to supply

disclosure of a claim element that is not expressly or inherently present in the reference.” See Consolidated Trial Practice Guide, at 36 (November 2019) (available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>).

Petitioner also contends that “a POSITA would understand that risk is a function of threats exploiting vulnerabilities to obtain, damage, or destroy assets—i.e., threat modeling is used to identify risks.” Pet., 23 (citations omitted). Petitioner contends that Keenan “visually depict[s] threats against IOE objects and creat[es] ‘Views’ through threat vectors, which may be combined with other Views, such as ‘model risk.’” Pet., 24.

But these arguments deviate improperly from what Keenan discloses about “risk,” which does not identify any “threats” as claimed. Keenan refers to the “risk” as a property. Keenan, 1:42 (“[t]hese properties (e.g. costs, risks and accountability)”). Keenan also refers to the risk as a “value.” For example, in Table 3 in its specification, Keenan discloses that the PALETTE view name includes an option called Model Risk. Keenan, 14:32-38. Under this view and option, an object shape’s color is “based on the *value* of the risk characteristics for the models in the view.” *Id.* (emphasis added). Keenan also refers to “risk” as a characteristic that is “preset.” Keenan, 16:4-5. Keenan views may “fill[] the object shapes based on the *value* of the technical risk ranking characteristics of that object.” Keenan, 16:21-23 (emphasis added). These disclosures support only that

“risk” in Keenan is a preset value as property of an object, and does not identify any “threats” as claimed.

Petitioner cites heavily to Keenan, 16:40-51, to argue that Keenan’s risk constitutes the claimed “threats.” But considered in full, this paragraph confirms the opposite. Keenan discloses:

In the example of FIG. 7, a Model Risk view 702 uses color to represent a range of risk based on the risk characteristics for models in the view.

A Business Affiliation view 704 uses color to represent differences in accountability for different business departments. A Business Unit view 706 uses color to represent business division accountability. A Technical Risk Measurement view 708 uses color to represent different types of risk (e.g., cyber, environmental, accidental, etc.). An Allocated Business Contribution view 710 uses color to represent aggregate attribution of business value to production chains (e.g., to indicate objects contributing to multiple business uses).

Keenan, 16:40-51. This disclosure indicates that different views display colors according to different properties. But risk is nothing more than a value or “metric” in Keenan (*id.*, 17:50), and does not disclose anything about any threats associated with any object. Indeed, Keenan discloses using the risk values in formulas to calculate aggregate risk, therefore confirming that risk is simply a number, and

neither discloses nor informs anything about any “threats” as claimed. As disclosed, Keenan allows a user to “calculate the risk of the selected View,” and even the “Calculate Aggregate risk by View” report “depicts risk values of the objects of the View aggregated based on an *aggregation formula*.” Keenan, 18:6-8, 18:20-22 (emphasis added).

Keenan's alerts can inform an owner of a change in risk, but this is also based on formulas and values, not “threats.” Keenan discloses that “[c]hanges to characteristics can also include formulas that calculate risk parameters based on new raw values put into ... characteristics of one object but flow downstream to other objects.” Keenan, 20:34-37. “Entire paths are preferably monitored for changes to aggregate characteristics values.” Keenan, 20:37-38. This disclosure indicates that a risk value or parameter can be changed by a user, *e.g.*, from 5 to 6, and that new value can require recalculations of the formulas using that value as an input. But once again, Keenan's risk is a numeric value as a property or characteristic, but does not disclose any “threats” as claimed.

Highlighting Keenan's failure to disclose any “threats” as claimed, Keenan fails to disclose how the risk value is computed or what the risk represents. At best, Keenan discloses that color can “represent different types of risk (*e.g.*, cyber, environmental, accidental, etc.).” Keenan, 16:40-51. But use of a color

identifying the generic nature of a risk still fails to disclose any threats associated with the risk.

This failure also appears in Petitioner's evaluation of Element 1[i]:

“generating ... and displaying ... a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.” Petitioner points to the disclosure of “Reports” in Keenan's Figure 1, and alleges that “Keenan's report displays each threat because the characteristics, *i.e.*, ‘risk characteristics,’ may be ‘converted into a Report,’ as well as because Keenan allows for specialized ‘Lasso reports,’ that allow for user-selected reports.” Pet., 40. But Keenan discloses no “threats” as claimed in any Lasso report, and does not generate or a display any report displaying any “threats.” Even Figure 16 of Keenan, which illustrates an exemplary Lasso Report, displays no threats, and Petitioner identifies none. See Pet., 40-41. At most, Figure 16 identifies the term “Threat Vector” in the text box, but per Keenan, a “Technical Threat Vector” uses color to fill “the object shapes based on the *value* of the technical risk ranking characteristic of that object.” Keenan, 16:21-23 (emphasis added). A report displaying a color associated with a value does not disclose any “threats” as claimed.

Because Keenan's use of the term "risk" fails to disclose any "threats" as claimed, Keenan does not and cannot anticipate any of the challenged claims. This Ground fails.

B. Keenan Also Fails to Disclose any "Mapping Files" as Claimed

Claim 1 also recites, in relevant part, "providing one or more mapping files communicatively coupled with the one or more databases," where "the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter 'third party diagram components')." Keenan "maps Visio shapes and formats to IOE shapes and formats." Keenan, 18:36-40. However, Keenan does not disclose a mapping file, and discloses only that the IOE "represents a dynamic map." Keenan, 5:27-44. Despite listing an extensive string of Keenan citations, Petitioner identifies no "mapping files" as claimed. Pet., 29. Though not permitted under a theory of anticipation, Petitioner improperly relies on expert testimony to manufacture the claimed "mapping files" in Keenan where none is disclosed. *Id.*

Indeed, Keenan's process has no need or use for any "mapping files" as claimed. Keenan discloses that when a user "selects the import function in the IOE GUI," Keenan "first checks to see if object already exists in IOE based on external ID number first, then name match." Keenan, 18:36-40. "To add an object[] directly to the IOE, the modification mode of the GUI includes a screen for the

user to select a method for adding an object, such as External Object ID, Use, Business Affiliation, Name of owner, and Name of object.” Keenan, 18:51-55. “If the IOE returns a topology with the object(s) already stored that match the criteria the user entered,” the IOE offers additional options. Keenan, 18:55-60. These disclosures confirm that Keenan does not disclose any “mapping files” as claimed. Rather, the import function in Keenan simply asks a user to search the IOE for an object matching the “external ID number” or “name.” If no match is found, IOE allows a user to add the object to the IOE.⁷

Petitioner states that a “POSITA would understand that Keenan’s disclosure of a ‘map’ discloses a ‘mapping file’ because a mapping file is required to form a map.” Pet., 29. This argument rings of inherency, but lacks any of the necessary underpinning. There is nothing inherent about using a mapping file in order to map “Visio shapes and formats to IOE shapes and formats.” According to Keenan, a user searches to see whether a pre-existing object is stored in the IOE, without disclosing a stored correlation. No “one or more mapping files” is required for this search to occur.

⁷ As discussed in Section II.B above, the ’366 Patent discloses that where “one or more tables of the database are used for the mapping file(s), each table is, for the purposes of this disclosure, a ‘file.’” ’366 Pat., 38:40-42. Petitioner does not identify or rely on any “table” in Keenan to satisfy the claimed feature of a “mapping file.”

Finally, the remainder of Petitioner's string citations are off-point and do not remedy these defects of Keenan. These citations reflect instances in Keenan where the term "map" is used, even though the term is not used in a manner relevant to the claimed "mapping file." For example, Petitioner cites to portions of Keenan's column 11 and 12, where Keenan discloses a mini map 204. Pet., 29. But this is just a graphical map, "displaying a depiction of the topology." Keenan, 11:65-66. Nothing about Keenan's graphical display of a mini map 204 discloses the existence of any "mapping files" as claimed, namely "one or more mapping files correlating the threat model components with visual diagram components of a third party software application."

As such, Keenan does not expressly disclose any "mapping files" as claimed, and "one or more mapping files" is neither required nor inherently disclosed by Keenan. Petitioner's reliance on Keenan as an anticipation reference is wrong and should be rejected.

C. Zheng Alone or in Combination with Secondary References Fails to Disclose any "Mapping Files" "Correlating the Threat Model Components with Visual Diagram Components of a Third Party Software Application"

Petitioner's Ground 2 challenge based on the "References of Ground 2" also fails to disclose every feature of the challenged claims. As already introduced above, claim 1 recites, in relevant part, "providing one or more mapping files communicatively coupled with the one or more databased, the one or more

mapping files correlating the threat model components with visual diagram components of a third party software application.”

In Ground 2, Petitioner initially relies upon Zheng to disclose “mapping techniques and concepts” and “one-to-one mapping between a threat actor and a threat target.” Pet., 63 (quoting Zheng, 3:24-34, 5:18-24). Petitioner then concludes that a “POSITA would understand that Zheng’s ‘mapping techniques’ and its ‘map’ convey, and necessarily include, a ‘mapping file’ as claimed because a mapping file would be required to perform mapping techniques.” Pet., 63 (citing Ex. 1003, ¶162). However, Zheng’s “mapping techniques” are related to visualization of the application architecture, “like cartography,” and have nothing to do with “correlating the threat model components with visual diagram components of a third party software application” as claimed. Zheng, 3:24-34. Zheng’s generic disclosure of “mapping techniques ... in the context of data visualization” does not necessarily require any “mapping files” as claimed.

Further, as already established in Section IV.B above, a mapping file is neither inherent nor required for a visualization or mapping between actor and target as described in Zheng. Petitioner’s declaration-based fabrication of a mapping file where none exists is improper in an IPR, where the claimed elements must be identified in a patent or printed publication. See 35 U.S.C. § 311(b); Consolidated Trial Practice Guide, at 36.

Petitioner’s improper challenge is not limited to its manufacture of the claimed “mapping files” based solely on Zheng’s use the term “mapping.”

Petitioner next modifies the non-existent mapping file without any support or motivation in the cited references and based solely on impermissible hindsight.

The sole mapping association Petitioner points to in Zheng is a “one-to-one mapping between a threat actor and a threat target.” Pet., 63 (quoting Zheng, 5:18-24). Even assuming Zheng disclosed a mapping file to associate a threat actor and a threat target—which it does not—Zheng does not disclose any mapping file “correlating the threat model components with visual diagram components of a third party software application” as claimed. Petitioner looks to Baker’s disclosure of “flowcharts [that] may be imported at step 104 from third party software such as that marketed as Microsoft Office Visio®.” Pet., 64 (quoting Baker, [0025]) (emphasis omitted). Petitioner then modifies the mapping file that it added to Zheng, and repurposes that undisclosed mapping file “to map between elements of the two software applications.” Pet., 64-65 (citing but not explaining Ex. 1004⁸, [0023]; Ex., 1003, ¶164). Petitioner states that a “POSITA would combine this teaching from Baker with the system of Zheng to enable the importation of diagrams from Microsoft Visio into the threat modeling software of Zheng such

⁸ This citation appears to be error, and should have been Ex. 1006, Baker, not Ex. 1004, Keenan. Either way, it is unfounded.

that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams.” Pet., 65. But again, Zheng does not disclose any mapping file, either expressly or inherently, and even considered in view of Baker, fails to disclose or suggest the claimed “mapping files” correlations. Much like Keenan, Baker’s process has no need or use for any “mapping files” as claimed. Baker stores the “text and shape of each element of the flowchart ... in the process database 30” and “automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts.” Baker, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as recited in the claims.⁹

As such, in order to reach the claimed “mapping files” correlations recited in claim 1, Petitioner first has to invent a mapping file to capture the threat actor/threat target association of Zheng, and then has to invent a modification to repurpose the associations. The sole motivation for these additions are hindsight-based creations of features not disclosed or suggested by the art. The References

⁹ As discussed in Section II.B above, the ’366 Patent discloses that where “one or more tables of the database are used for the mapping file(s), each table is, for the purposes of this disclosure, a ‘file.’” ’366 Pat., 38:40-42. Petitioner does not identify any such “table” in Baker, and does not rely on any such “table” to satisfy the claimed feature of a “mapping file.”

of Ground 2 fail to disclose any “mapping files” possessing the claimed correlations.

This failure also taints Petitioner's analysis of Element 1[g]: “determining using the one or more computing devices, for the subset of third party diagram components, correlated threat model components as defined in the one or more mapping files.” Petitioner asserts that “Zheng discloses ‘determining ... for the subset of third party diagram components, correlated threat model components,’ because Zheng discloses a ‘map’ that defines relationships between the third party components and among other system components.” Pet., 68 (citing Zheng, 2:38-42). But Zheng's disclosure of a map, *i.e.*, a visualization “like cartography” (Zheng, 3:24-34), does not support Petitioner's contention regarding the claimed use of “mapping files” for “determining ... correlated threat model components.” Further, Zheng's disclosure of mapping between target and actor does not satisfy this claim element, which is directed instead to correlations between third party diagram components and threat model components. These claimed features of Element 1[g] are neither disclosed nor suggested by the References of Ground 2.

D. Grounds 3-5 Fail to Remedy the Above-Identified Failures of Grounds 1 and 2

Grounds 3, 4, and 5 are not presented to address the defects in Keenan and Zheng (alone or in combination with the other References of Ground 2) as discussed above. Rather, these defects infect each of the asserted grounds. For

example, in Ground 3, Galliano is relied upon for the challenges of dependent claims 2, 9 and 17, but Galliano does not remedy (and is not relied upon to remedy) the defects of Ground 2. Pet., 85-87. Similarly, in Ground 4, Keenan is added to the References of Ground 2, but to challenge claims 5-6, 12-14, and 19-20, not to remedy the failure in Ground 2 to establish the disclosure or suggestion of the “mapping files” as claimed. Pet., 87-88. Ground 5 adds the knowledge of a POSITA to the References of Ground 2, but to challenge claims 2, 5-6, 9, 12-14, 17, and 19-20, not to remedy Ground 2's failure to establish the disclosure or suggestion of the “mapping files” as claimed. Pet., 88-89. Further, Ground 5 violates the statutory requirement that IPR challenges be based upon patents and printed publications. See 35 U.S.C. § 311(b).

V. CONCLUSION

For the reasons presented above, no *inter partes* review should be instituted.

Dated: July 12, 2023

/s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
NOSSAMAN, LLP
1401 New York Ave, NW
Suite 800
Washington, DC 20005
Telephone: (202) 887-1400
Email: whelge@nossaman.com

IPR2023-00656 Patent Owner's Preliminary Response

James T. Wilson (Reg. No. 41,439)
DAVIDSON BERQUIST JACKSON &
GOWDEY, LLP
8300 Greensboro Dr., Suite 500
McLean, VA 22102
Telephone: (571) 765-7700
Fax: (571) 765-7200
Email: jwilson@dbjg.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing PATENT OWNER'S PRELIMINARY RESPONSE complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the brief contains 5,805 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

By: /s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
Attorney for Patent Owner

CERTIFICATE OF SERVICE

I hereby certify that on July 12, 2023, a true and correct copy of the foregoing document was served via email, by consent, to Petitioner by serving the correspondence email addresses of record as follows:

Brent Yamashita
Reg. No. 53,808
DLA Piper LLP (US)
2000 University Avenue
East Palo Alto, California
94303-2214
Phone: 650.833.2348
Fax: 650.833.2001
Email:
brent.yamashita@us.dlapiper.com

Blake Jackson
Reg. No. 66,272
DLA Piper LLP (US)
2000 University Avenue
East Palo Alto, California
94303-2214
Phone: 650.833.2248
Fax: 650.687.1148
Email:
blake.jackson@us.dlapiper.com

Matthew Middleton
Reg. No. 77,117
DLA Piper LLP (US)
1201 N. Market St., Suite 2100
Wilmington, Delaware
19801-1147
Phone: 302.468.5675
Fax: 302.778.7935
Email:
matthew.middleton@us.dlapiper.com

/s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
Attorney for Patent Owner