

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner

v.

THREATMODELER SOFTWARE INC.,
Patent Owner

IPR2023-00656

U.S. Patent No. 10,713,366

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,713,366
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	2
II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(b)(1)-(4)	2
A. Real Parties-In-Interest.....	2
B. Related Matters.....	2
C. Counsel	3
D. Service Information.....	3
III. STANDING	4
IV. PAYMENT OF FEES – 37 C.F.R. § 42.103.....	4
V. TECHNOLOGY BACKGROUND.....	4
VI. SUMMARY OF THE '366 PATENT	6
A. Brief Description	6
B. Priority Date	8
C. Prosecution History of '366 Patent	8
VII. IDENTIFICATION OF CHALLENGES UNDER 37 C.F.R. § 42.104(B).....	10
A. Prior Art.....	10
B. Challenges	11
VIII. LEVEL OF ORDINARY SKILL IN THE ART.....	12
IX. CLAIM CONSTRUCTION	12
A. “Third-Party Software Application”	13
B. “Third Party Diagram Components” and “Visual Representations of the Threat Model Components”	13
C. “Threat Model Components”	14
X. DETAILED EXPLANATION AND SUPPORTING EVIDENCE.....	14
A. Overview of the Prior Art.....	14
1. Keenan.....	14
2. Zheng.....	17

3.	Baker	18
4.	Jones.....	19
5.	Galliano	20
B.	Ground 1: Keenan Anticipates Claims 1-20	21
1.	Claim 1	21
a.	Element 1[p]. “A threat modeling method, comprising:”	21
b.	Element 1[a]. “providing one or more databases, the one or more databases comprising:”	24
c.	Element 1[b]. “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;”	25
d.	Element 1[c]. “providing one or more mapping files communicatively coupled with the one or more databases,”	29
e.	Element 1[d]. “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”); and”	30
f.	Element 1[e]. “in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:”	32
g.	Element 1[f]. “using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”	34

h.	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;”	35
i.	Element 1[h]. “displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”	36
j.	Element 1[i]. “generating, using the one or more computing devices, and displaying, on the one or more user interfaces, 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.”	39
2.	Claim 2: “The method of claim 1, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”	41
3.	Claim 3: The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.....	42
4.	Claim 4: “The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file.”	42

5. Claim 5: “The method of claim 1, wherein determining, for the subset of third party diagram components, correlated threat model components, comprises first determining whether a user-defined name for one of the subset of third party diagram components has a match in the one or more mapping files and, if no match is found, then determining whether a default title for the third party diagram component, as defined by the third party software application, has a match in the one or more mapping files.” 43
6. Claim 6: “The method of claim 5, further comprising, if no match is found for the default title, matching the third party diagram component with a placeholder component and displaying the placeholder component on the relational diagram to indicate that no match was found.” 44
7. Claim 7: “The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files.” 47
8. Claim 8: 48
 - a. Element 8[p]. “A threat modeling system, comprising: one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:” 48
 - b. Element 8[a]. “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;” 48
 - c. Element 8[b]. “one or more mapping files communicatively coupled with the one or more databases, 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”);” 48

- d. Element 8[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by one of the one or more computing devices, the data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;” 48
- e. Element 8[d]. “an interface configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files;” 51
- f. Element 8[e]. “a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and” 52
- g. Element 8[f]. “a threat report interface, displayed on the one or more computing devices, including 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.” 54
- 9. Claim 9: “The system of claim 8, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.” 54
- 10. Claim 10: The system of claim 8, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.....54

11. Claim 11: “The system of claim 8, wherein the data file comprises one of a VSD file, a VSDX file, a TMT File, an XML file, a JSON file, a PNG file, and a JPEG file.” 55
12. Claim 12: “The system of claim 8, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components.” 55
13. Claim 13: “The system of claim 8, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.” 56
14. Claim 14: The system of claim 8, wherein, for each of the subset of third party diagram components for which no correlated threat model component is found in the one or more mapping files, the diagram interface displays a placeholder component indicative of a match not being found. 56
15. Claim 15: The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files.....57
16. Claim 16:.....58
 - a. Element 16[p]. “A threat modeling system, comprising: one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:” 58
 - b. Element 16[a]. “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;” 58

- c. Element 16[b]. “one or more mapping files communicatively coupled with the one or more databases, 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”);” 58
- d. Element 16[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by the one or more computing devices, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;” 58
- e. Element 16[d]. “an interface configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files;” 58
- f. Element 16[e]. “a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of a computing network, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and” 59
- g. Element 16[f]. “a threat report interface, displayed on the one or more computing devices, including 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.” 59

17.	Claim 17: “The system of claim 16, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”	59
18.	Claim 18: The system of claim 16, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.....	59
19.	Claim 19: The system of claim 16, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components.....	59
20.	Claim 20: “The system of claim 16, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.”	60
C.	Ground 2: Zheng In View of Baker and Jones Renders Obvious Claims 1-4, 7-11, 15-18.....	60
1.	Claim 1	60
a.	Element 1[p]. “A threat modeling method, comprising:”	60
b.	Element 1[a]. “providing one or more databases, the one or more databases comprising:”	61
c.	Element 1[b]. “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;”	61
d.	Element 1[c]. “providing one or more mapping files communicatively coupled with the one or more databases,”	63
e.	Element 1[d]. “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”); and”	63

f.	Element 1[e]. “in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:”	65
g.	Element 1[f]. “using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”	66
h.	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;”	67
i.	Element 1[h]. “displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”	69
j.	Element 1[i]. “generating, using the one or more computing devices, and displaying, on the one or more user interfaces, 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.”	70
2.	Claim 2: “The method of claim 1, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”	73
3.	Claim 3: The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.	74

4. Claim 4: “The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file.” 74
5. Claim 7: “The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files.” 74
6. Claim 8:.....75
 - a. Element 8[p] (*see* Ground 1 for text of this element). 75
 - b. Element 8[a] (*see* Ground 1 for text of this element). 75
 - c. Element 8[b] (*see* Ground 1 for text of this element). 76
 - d. Element 8[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by one of the one or more computing devices, the data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;” 76
 - e. Element 8[d] (*see* Ground 1 for text of this element). 77
 - f. Element 8[e] (*see* Ground 1 for text of this element). 78
 - g. Element 8[f] (*see* Ground 1 for text of this element). 80
7. Claim 9 (*see* Ground 1 for text of this element). 81
8. Claim 10 (*see* Ground 1 for text of this element). 81
9. Claim 11 (*see* Ground 1 for text of this element). 81

10.	Claim 15: The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files.....	81
11.	Claim 16:.....	82
a.	Element 16[p]. (<i>see</i> Ground 1 for text of this element).	82
b.	Element 16[a]. (<i>see</i> Ground 1 for text of this element).	82
c.	Element 16[b]. (<i>see</i> Ground 1 for text of this element).	82
d.	Element 16[c]. (<i>see</i> Ground 1 for text of this element).	82
e.	Element 16[d]. (<i>see</i> Ground 1 for text of this element).	82
f.	Element 16[e]. (<i>see</i> Ground 1 for text of this element).	82
g.	Element 16[f]. (<i>see</i> Ground 1 for text of this element).	82
12.	Claim 17 (<i>see</i> Ground 1 for text of this element).	82
13.	Claim 18 (<i>see</i> Ground 1 for text of this element).	82
14.	A POSITA Would Have Been Motivated to Combine Zheng With Baker and Jones.	83
D.	Ground 3: The References of Ground 2 in Further View of Galliano Render Obvious Claims 2, 9, and 17.....	85
E.	Ground 4: The References of Ground 2 in Further View of Keenan Render Obvious Claims 1-20.....	87
F.	Ground 5: The References of Ground 2 in Further View of the Knowledge of a POSITA Render Obvious Claims 2, 5-6, 9, 12-14, 17, and 19-20.....	88

XI.	THIS PETITION IS PROPER UNDER 35 U.S.C. §§ 314(a) AND 325(d).....	89
A.	Stay	89
B.	Trial Date.....	89
C.	Parallel Proceeding.....	90
D.	Issue Overlap	90
E.	Same Party	90
F.	Other Considerations.....	91
XII.	CONCLUSION.....	91

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	89
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (PTAB May 15, 2020)	91
<i>Grp. - Trucking LLC</i> , IPR2019-01393, Paper 24 (June 16, 2020)	90
Statutes	
35 U.S.C. § 102(a)	10, 11
35 U.S.C. § 102(a)(1)	11
35 U.S.C. § 102(a)(2)	11
35 U.S.C. § 102(b)	10, 11
35 U.S.C. §§ 311-19	2
Other Authorities	
37 C.F.R. § 42.10(b)	3
37 C.F.R. § 42.15(a)	4, 5, 8, 9
37 C.F.R. § 42.100	2
37 C.F.R. § 42.104(a)	4

EXHIBITS

Exhibit No.	Description
EX-1001	U.S. Patent No. 10,713,366 (“the ’366 patent”)
EX-1002	Prosecution History of the ’366 patent
EX-1003	Declaration of Robert Hurlbut
EX-1004	U.S. Patent No. 11,200,228 (“Keenan”)
EX-1005	U.S. Patent No. 10,503,907 (“Zheng”)
EX-1006	U.S. Patent Pub. 2014/0236665 (“Baker”)
EX-1007	U.S. Patent No. 9,602,529 (“Jones”)
EX-1008	U.S. Patent No. 10,681,068 (“Galliano”)
EX-1009	Federal Judiciary Report
EX-1010	Email from Petitioner’s Counsel to PO’s Counsel
EX-1011	Excerpts from <i>Risk Centric Threat Modeling</i> , by Tony Uceda Velez and Marco M. Morana, John Wiley and Sons, Inc., 2015
EX-1012	Excerpts from <i>Threat Modeling Designing for Security</i> , by Adam Shostack, John Wiley and Sons, Inc., 2014
EX-1013	Excerpts from <i>Threat Modeling</i> , by Frank Swiderski and Window Snyder, Microsoft Press, 2004
EX-1014	Excerpts from <i>The Security Development Lifecycle</i> , by Michael Howard and Steve Lipner, Microsoft Press, 2006

I. INTRODUCTION

IriusRisk Inc. (“Petitioner”) requests *inter partes* review of claims 1-20 (the “Challenged Claims”) of U.S. Patent No. 10,713,366 (the “’366 patent,” EX-1001), owned by ThreatModeler Software Inc. (“PO”), pursuant to 35 U.S.C. §§ 311-19 and 37 C.F.R. § 42.100.

The ’366 patent relates to a computer application for generating a threat model. During prosecution, the ’366 patent was allowed because the prior art of record did not disclose the element involving the importation of diagrams from “a third party software application” into the threat model computer application. As explained below, that element, and all other elements of the Challenged Claims, are disclosed in the prior art discussed herein. None of that prior art was considered by the Examiner during prosecution.

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(b)(1)-(4)

A. Real Parties-In-Interest

Petitioner, as well as IriusRisk SL, are the real parties-in-interest.

B. Related Matters

PO has asserted the ’366 patent in the following litigation against Petitioner: *ThreatModeler Software Inc v. IriusRisk, Inc.*, C.A. No. 22-912-MN (D. Del.), for which the Complaint was served on July 8, 2022 (the “Litigation”). There, PO asserts the ’366 patent and related U.S. Patent No. 10,699,008 against Petitioner.

C. Counsel

Petitioner designates lead and back-up counsel as noted below. Powers of attorney pursuant to 37 C.F.R. § 42.10(b) accompany this Petition.

Lead Counsel	Backup Counsel
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

D. Service Information

Please address all correspondence to counsel at the address above. Petitioner consents to electronic service by email at:

brent.yamashita@us.dlapiper.com;

blake.jackson@us.dlapiper.com;

matthew.middleton@us.dlapiper.com.

III. STANDING

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '366 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review.

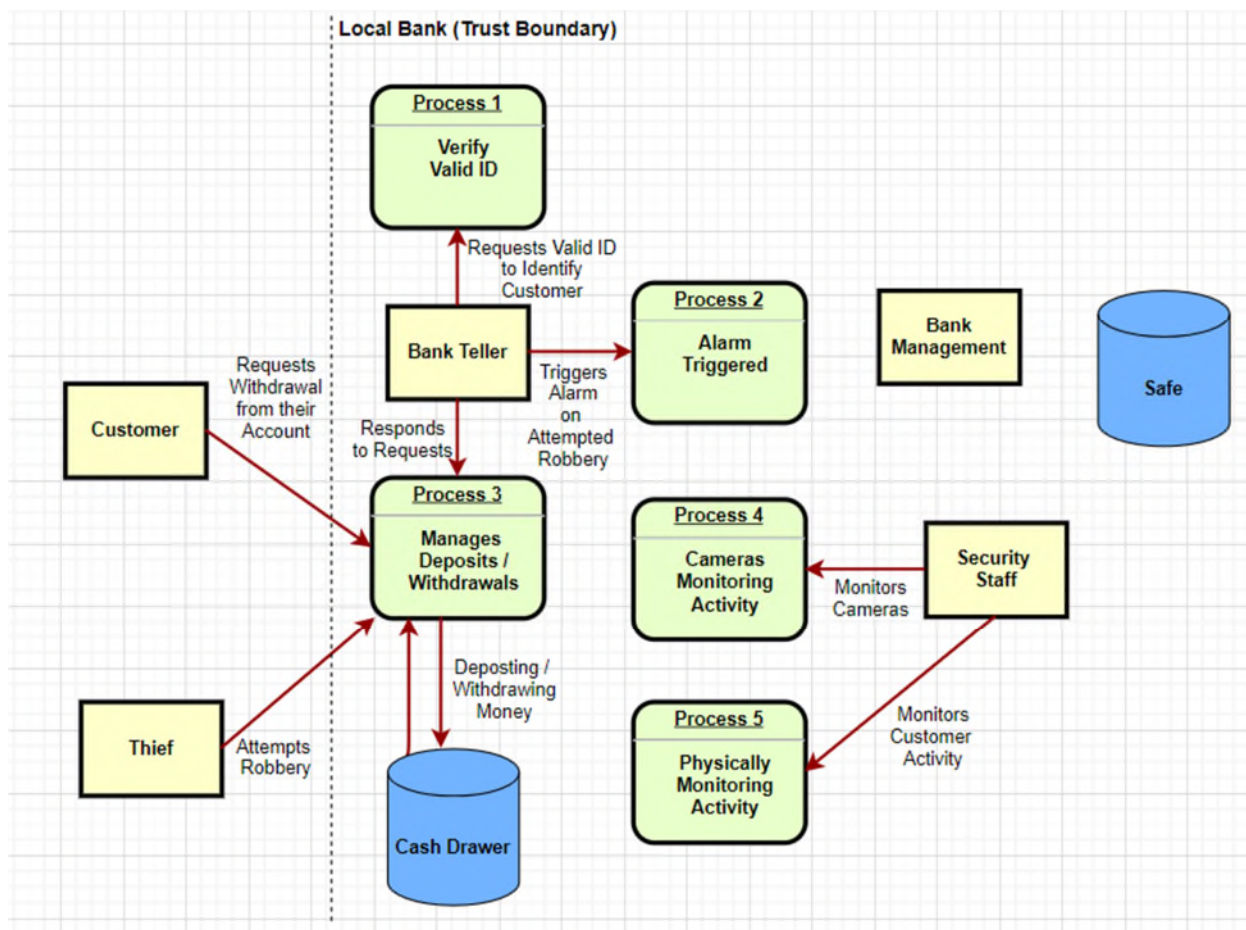
IV. PAYMENT OF FEES – 37 C.F.R. § 42.103

The undersigned authorizes the Director to charge the fee specified by 37 C.F.R. §42.15(a) and any additional fees that might be due in connection with this Petition to Deposit Account No. 50-3266.

V. TECHNOLOGY BACKGROUND

Threat modeling is a process by which potential threats to a system are identified. The system can be almost anything that is vulnerable to threats and that humans wish to protect, *e.g.*, a physical structure, such as an office building or a power plant, or a digital asset, such as financial data or customer information. EX-1003, ¶135.

A threat model is a useful tool for human beings to systematically understand a system's vulnerabilities. Historically, threat models were often developed by people drawing on a white board or a piece of paper and later could be prepared using computer software applications such as the Microsoft SDL Threat Modeling Tool, which the '366 patent admits is prior art. EX-1003, ¶135; EX-1001, 1:56-60. A simple example of a threat model is the following, which shows potential threats to physical branch of a bank:



EX-1003, ¶35.

This diagram, called a Data Flow Diagram, which is commonly used for Threat Modeling, depicts the following elements:

- **Actors:** Customer, Thief, Bank Teller, Bank Management, Security Staff
- **Processes:** Verify Valid ID, Manages Deposits / Withdrawals, Alarm Triggered, Camara Monitoring Activity, Physically Monitoring Activity
- **Data Stores or Assets:** Cash Drawer, Safe

- **Data Flows:** Arrows in the diagram to show actions or data flowing between Actors and Processes or between Processes and Data Stores or Assets

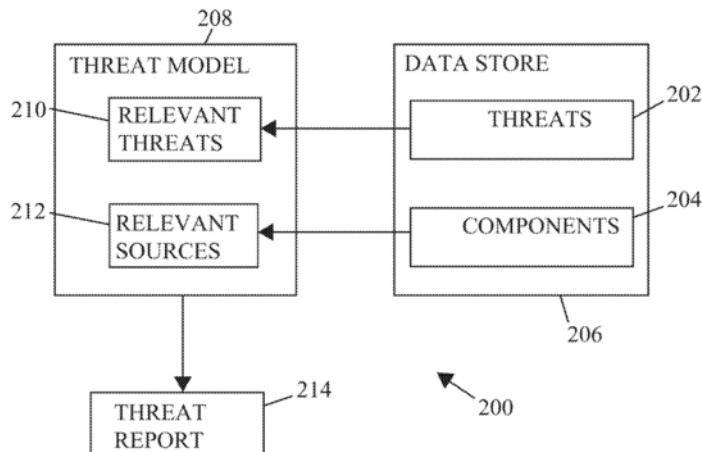
The Data Flow Diagram helps identify potential threat actors (Customer, Thief) and various countermeasures to create an initial threat model known in the art before the '366 patent's priority date. EX-2011-2014; EX-1003, ¶¶35-37.

VI. SUMMARY OF THE '366 PATENT

A. Brief Description

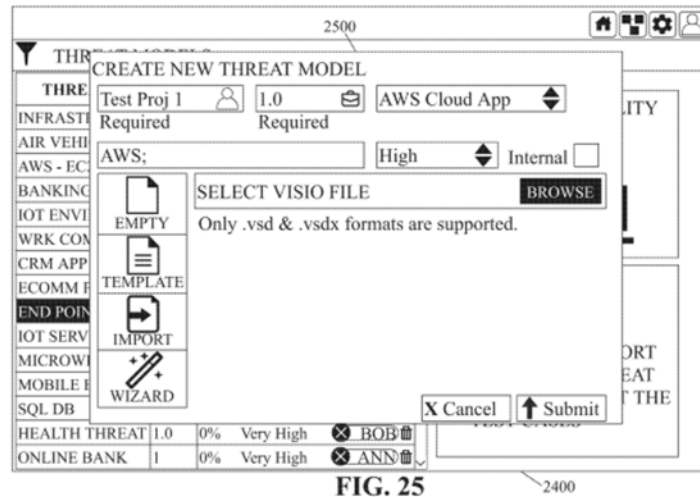
The '366 patent, entitled “Systems and Methods For Automated Threat Model Generation From Third Party Diagram Files,” relates to threat modeling. EX-1001. The patent explains that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” EX-1001, 1:56-57. Threat modeling involves the identification and visualization of potential threats, which typically involves generating diagrams on a whiteboard or in a computer application to represent the potential threats to a particular system. EX-1003, ¶38.

The '366 patent describes that threat models are created from defined threats and threat model components, which are stored within a database. EX-1001, 9:10-16. This is shown in Figure 2:



Each threat model component “is a potential relevant source for one or more threats.” EX-1001, 9:55-10:7; EX-1003, ¶39.

The ’366 patent further describes creating diagrams in a “third party software application” such as Microsoft Visio and using those diagrams in the threat model. *Id.*, 24:26-29. The patent describes a mapping file that components from those diagrams with threat model components. EX-1001, 37:14-18, 37:25-39. Figure 25 depicts an interface by which a user imports a diagram from Microsoft Visio:



EX-1003, ¶¶40-42.

The threat /model system also can generate a threat report, which can identify threats, the status of threats, and the sources of threats, among other things.” EX-1001, 9:6-9; EX-1003, ¶43.

B. Priority Date

The ’366 patent claims priority to four provisional applications, the earliest of which was filed on May 17, 2017. For the purposes of this IPR only, Petitioner applies a priority date of May 17, 2017.

C. Prosecution History of ’366 Patent

The ’366 patent was filed on August 15, 2019. EX-1002, Application. In an Office Action dated November 18, 2019, the Examiner rejected all pending claims as indefinite. *Id.*, Office Action (“OA”) at pp. 3-6. The Examiner found that “a person of ordinary skill in the art would not be able to determine how the claimed ‘visual representations’ relate to the ‘third party diagram components,’” where the

third-party diagrams themselves are visual representations. *Id.*, OA at p. 4. During an interview following the rejection, Applicant represented that the “third party diagram components” and “visual representations of the threat model components” were distinct elements. *Id.*, Response to Office Action dated November 18, 2019 (“Response”) at p. 8.

The Examiner also rejected claims 1, 5, 6, 8, 12-14, 19-20 for uncertainty due to the use of the term “third party components,” noting that “third party” “refers to an issue of ownership, which can change at arbitrary times.” *Id.*, OA at pp. 5-6. During the interview, Applicant and Examiner agreed that “third party” would not necessarily indicate present ownership, but rather “independently-created software applications not created with a common schema, such that a mapping file or the like as claimed in the claims would be useful to map between elements of the two software applications.” *Id.*, Response at pp. 9-10.

Based on the interview and associated claim amendments, the Examiner withdrew all rejections and issued a notice of allowance. *Id.*, Notice of Allowance (“NOA”). As reasons for allowance, the Examiner noted that the prior art of record did not disclose “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.” *Id.*, NOA at pp. 2-3. Moreover, the Examiner found that the prior art of record did not disclose “third-party control of

the diagram components of the architecture model, wherein ‘the one or more mapping files correlating the threat model components with ***visual diagram components of a third party software application.***’ *Id.* (emphasis added).¹

Notably, the prior art relied upon in this petition—which was not disclosed during prosecution or considered by the Examiner—discloses all elements of the Challenged Claims including the ability to import a diagram from a third-party software application. EX-1001, cover page; EX-1003, ¶¶46-51.

VII. IDENTIFICATION OF CHALLENGES UNDER 37 C.F.R. § 42.104(B)

A. Prior Art

The challenges in this Petition are based on the knowledge of a person of ordinary skill in the art (a “POSITA”) and the following:

- **Keenan (EX-1004):** U.S. Patent No. 11,200,228 (“Keenan”) was filed on April 19, 2018, and issued on December 14, 2021. Keenan claims priority to April 19, 2017. Keenan is prior art to the ’366 patent under 35 U.S.C. § 102(a)(2).
- **Zheng (EX-1005):** U.S. Patent No. 10,503,907 (“Zheng”) was filed on December 14, 2016, published on June 15, 2017, and

¹ Unless indicated otherwise, all emphasis in quotations contained herein has been added.

claims priority to December 14, 2015. Zheng is prior art under 35 U.S.C. § 102(a)(2).

- **Baker (EX-1006):** U.S. Patent Pub. No. 2014/0236665 (“Baker”) was published on August 21, 2014 and is prior art under 35 U.S.C. § 102(a)(1).
- **Jones (EX-1007):** U.S. Patent No. 9,602,529 (“Jones”) was published on October 8, 2015. Jones is prior art under 35 U.S.C. § 102(a)(1).
- **Galliano (EX-1007):** U.S. Patent No. 10,681,068 (“Galliano”) was filed on January 4, 2017, and claims priority to July 26, 2016. Galliano is prior art under 35 U.S.C. § 102(a)(2).

B. Challenges

Petitioner requests cancellation of claims 1-20 of the ’366 patent based on the following grounds:

Ground	Claims	Basis	Reference(s)
1	1-20	§102	Keenan
2	1-4, 7-11, 15-18	§103	Zheng in view of Baker and Jones
3	2, 9, and 17	§103	The references of Ground 2 in further view of Galliano
4	1-20	§103	The references of Ground 2 in further view of Keenan
5	2, 5-6, 9, 12-14, 17, 19-20	§103	The references of Ground 2 in further view of the knowledge of a POSITA

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A POSITA as of the filing date of the '366 patent would have had a Bachelor's degree in computer engineering, computer science, mathematics, or a similar discipline, with at least three years of relevant industry or research experience, including experience in software development and designing or implementing threat models. Additional work or research experience can substitute for less or different education, and vice-versa. EX-1003, ¶33.

IX. CLAIM CONSTRUCTION

The Challenged Claims are interpreted using the same standard used in federal district court. PO defined certain claim terms in the specification and file history, as described below. Petitioner is applying those definitions in this petition. For all other claim terms, Petitioner applies the plain and ordinary meaning that a POSITA would attribute to those terms.

A. “Third-Party Software Application”

As discussed *supra* Section VI.C., to overcome an indefiniteness rejection, Applicant stated that the term “third party” did not necessarily indicate ownership and expressly defined “third party software applications” to mean “independently-created software applications not created with a common schema, such that a mapping file or the like as claimed in the claims would be useful to map between elements of the two software applications.” EX-1002, Response at pp. 9-10; EX-1003, ¶53.

Applicant further made clear through the use of examples that commonly-owned software can still be “third party” software where the applications are not created with a common schema and thus the use of a mapping file as claimed would still be useful. EX-1002, Response at pp. 10-11; EX-1003, ¶¶53-54.

B. “Third Party Diagram Components” and “Visual Representations of the Threat Model Components”

Applicant made further representations in the file history, representing that “the third party diagram components [are] components of an independent software application,” and that “visual representations of the threat model components [are] components of the native software, stored in databases/servers locally or remotely but coupled with the system.” EX-1002, Response at p. 8; EX-1003, ¶55.

C. “Threat Model Components”

Based on the specification, the term “threat model components” means “a potential relevant source for one or more threats.” Referring to FIG. 2, the patent explains that a threat model “component” is “a potential relevant source for one or more threats,” stating “[f]or example, one threat may be Bluejacking and one component, which would be correlated to this threat through the database, could be “Bluetooth port.” EX-1001, 9:55-59; EX-1003, ¶¶56-60.

X. DETAILED EXPLANATION AND SUPPORTING EVIDENCE

Keenan anticipates all Challenged Claims. Keenan expressly discloses importing a diagram from Microsoft Visio, which is the primary example of a third-party software application disclosed in the ’366 patent. For completeness, Petitioner also presents four obviousness grounds.

A. Overview of the Prior Art

1. Keenan

Keenan discloses threat modeling with “an Integrated Object Environment (IOE) running in a graph database environment.” EX-1004, Abstract. The described threat modeling systems and methods “include storing, revealing and *maintaining value and risk of information assets*, such as the topology of an analytical infrastructure in query-driven, graph database.” *Id.* The IOE “stores, reveals and links characteristics (Structural Metadata) of each object in the topology either within the IOE or in a linked repository, such that accountability,

benefits and consequences of using those assets can easily and repeatedly be measured.” *Id.*, 1:47-52. A user may interact with the IOE through a Graphical User Interface (GUI), including “a View mode, where the user can view any section of the topology and Characteristics by Object” and “a Modify mode, where the user can add, change and delete Objects or Characteristics.” *Id.*, 11:42-51. “The intelligence embedded in the stored topology can be viewed in a variety of ways through the GUI, both in terms of the object-to-object relationships and the associated characteristics of objects,” *id.*, 12: 64-67, including processing and viewing objects by threat vectors, which “fills the object shapes based on the value of the ***technical risk*** ranking characteristics of that object,” where the Views can be viewed in combination with one another, *id.*, 16:21-23, 14:7-15:10 (Table 3), Fig. 16.

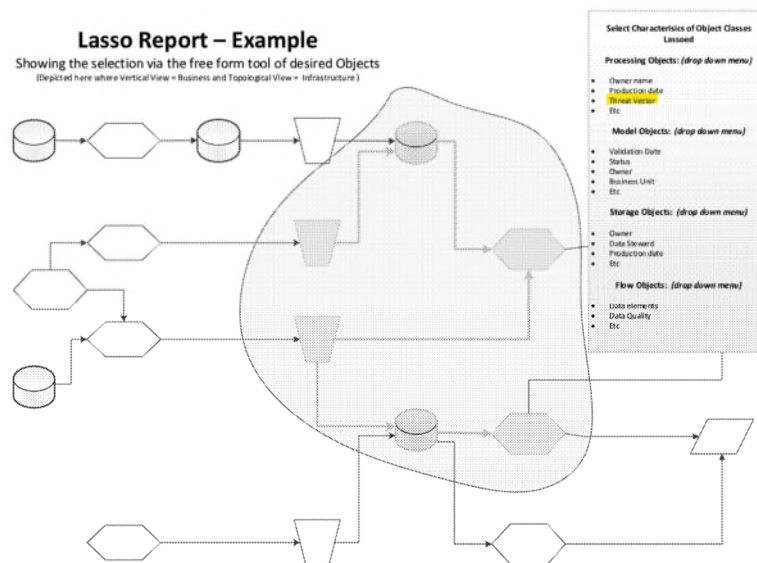


FIGURE 16

“The major components of the IOE appear in FIG. 1. In general, each real world component in the infrastructure is defined as an object with associated characteristics such as state, and its relationship to other objects. The objects and characteristics are stored in a graphical format 102 such as a Visio file. **The system converts the Visio files 102 into a standard, canonical format for storage in a topology graph database 104 of the infrastructure.** Alternatively, a GUI 106 is provided for inputting directly into the topology database. Rendering software (GUI) 106 converts the graph database and associated characteristics into Views, which are exportable as diagrams 108, as well as **reports 110** and alerts 112.” *Id.*, 5:27-44.

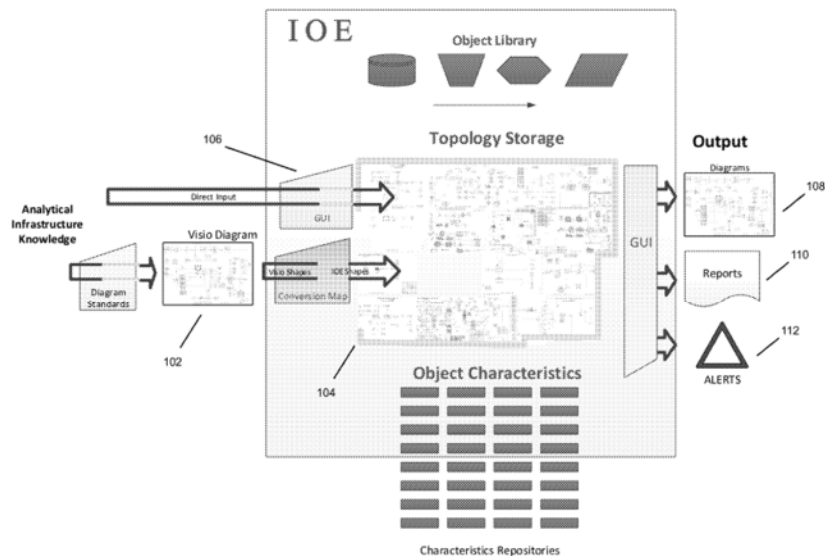


FIGURE 1

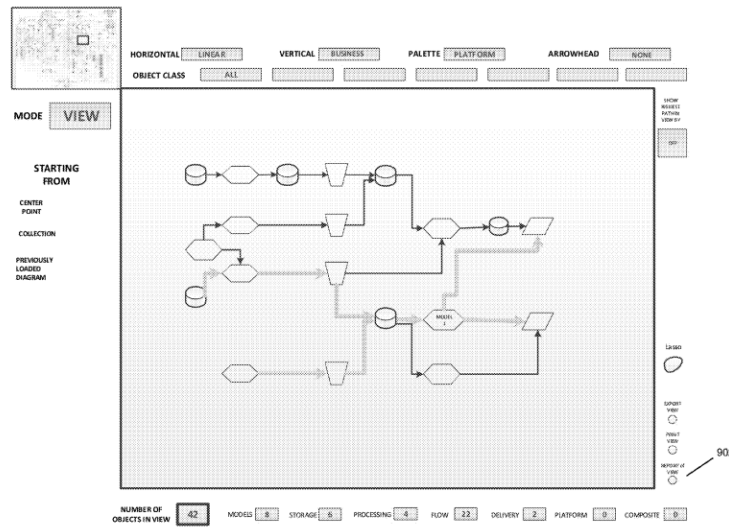


FIGURE 9

Id., Figs. 1, 9.

As shown in, *e.g.*, Fig. 1, “[a] map is preset that **maps Visio shapes and formats to IOE shapes and formats**. The user selects the **import function** in the IOE GUI, which first checks to see if object already exists in IOE based on external ID number first, then name match. If the object already exists, a message is posted to the screen, such as, ‘The following objects matched existing objects from the IOE, new relationships will be loaded to existing object.’ The existing Objects are then updated with new relationships based on **the imported Visio diagram**.” *Id.*, 18:36-50; EX-1003, ¶¶62-65.

2. Zheng

Zheng is titled “Intelligent Threat Modeling and Visualization” and discloses “[a] computer-implemented system... for visualizing and **analyzing security threats** in a suite of software applications.” EX-1005, Abstract. “The system

includes ***a visualization module*** for rendering, on a computer display, ***a map with components*** representative of the suite of software applications and relationships among the software applications.” *Id.* “***The threat modeling module*** is adapted to interact with the visualization module to ***graphically depict*** on the computer display the one or more ***security threats on the map in a threat modeling layer.***” *Id.*; EX-1003, ¶¶66-69.

3. Baker

Baker discloses threat modeling and is relied upon in this Petition for its express description of importing figures from third-party software, Microsoft Visio: “risk management or control flowcharts ***may be imported at step 104 from third party software such as that marketed as Microsoft Office Visio®.***” EX-1006 at paragraph 0025, as shown in Fig. 4:

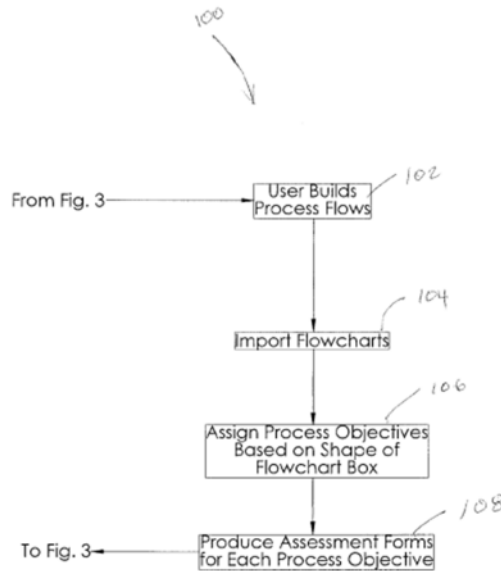


Fig. 4

EX-1003, ¶¶70-72.

4. Jones

Jones discloses threat modeling and is relied upon in this Petition for its disclosure of threat reports. For example, Jones discloses: “The reporter 114 may be configured to generate one or more reports from the threat analysis, at least one of which may include an organized arrangement of at least some of the attributes of at least some of the components, data flows or cybersecurity threat.” EX-1007, 6:59-63. Figure 5 discloses Report Generator 502:

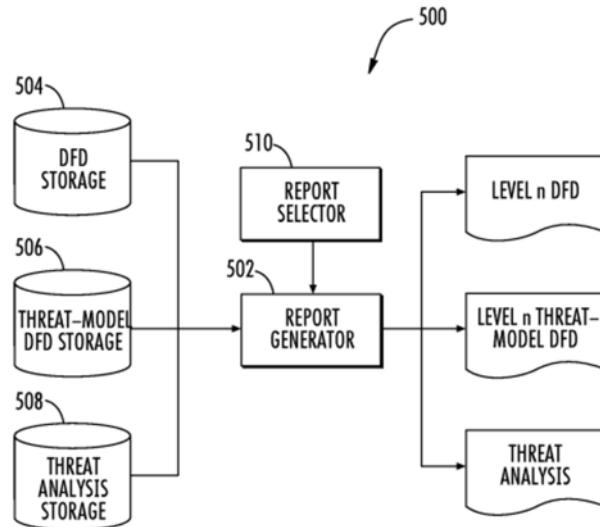
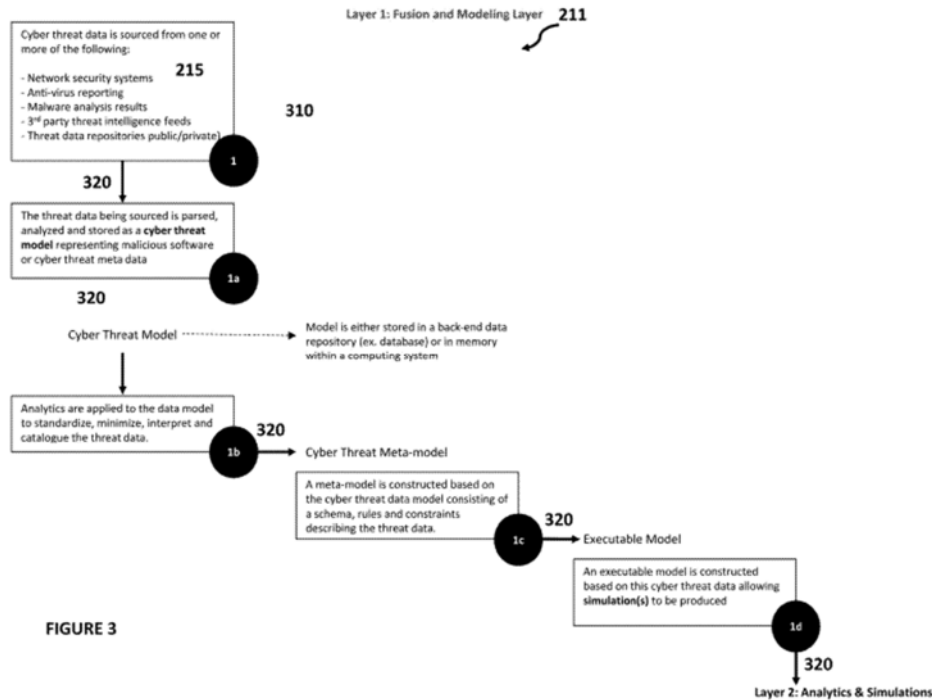


FIG. 5

EX-1003, ¶¶73-74.

5. Galliano

Galliano discloses threat modeling and is relied upon in this Petition for its description of storing a threat model in a database or a computing system, as described in Figure 3:



EX-1008, Figure 3; EX-1003, ¶¶75-76.

B. Ground 1: Keenan Anticipates Claims 1-20

Keenan discloses every element of claims 1-20. EX-1003, ¶77; *see also id.*, Exhibit B.

1. Claim 1

a. Element 1[p]. “A threat modeling method, comprising:”

To the extent the preamble is limiting, Keenan discloses this element. EX-1003, ¶¶78-79. Keenan discloses an Integrated Object Environment (“IOE”) with a Graphical User Interface (“GUI”) “which allows the user *a quick way to calculate the risk* of the selected View,” as well as generate risk reports, where “[e]xamples of those risk reports include: *Aggregate Model Risk of the View*,

which calculates the **aggregate model risk** for all models in the View.” EX-1004, 18:6-13; *see also, e.g.*, Abstract, 4:64-67, 7:41-59, 13:4-22, 14:35-39, 14:61-63, 16:1-29, 16:40-5, 17:32-40, 18:6-13, 20:34-5, Figs. 7, 16.

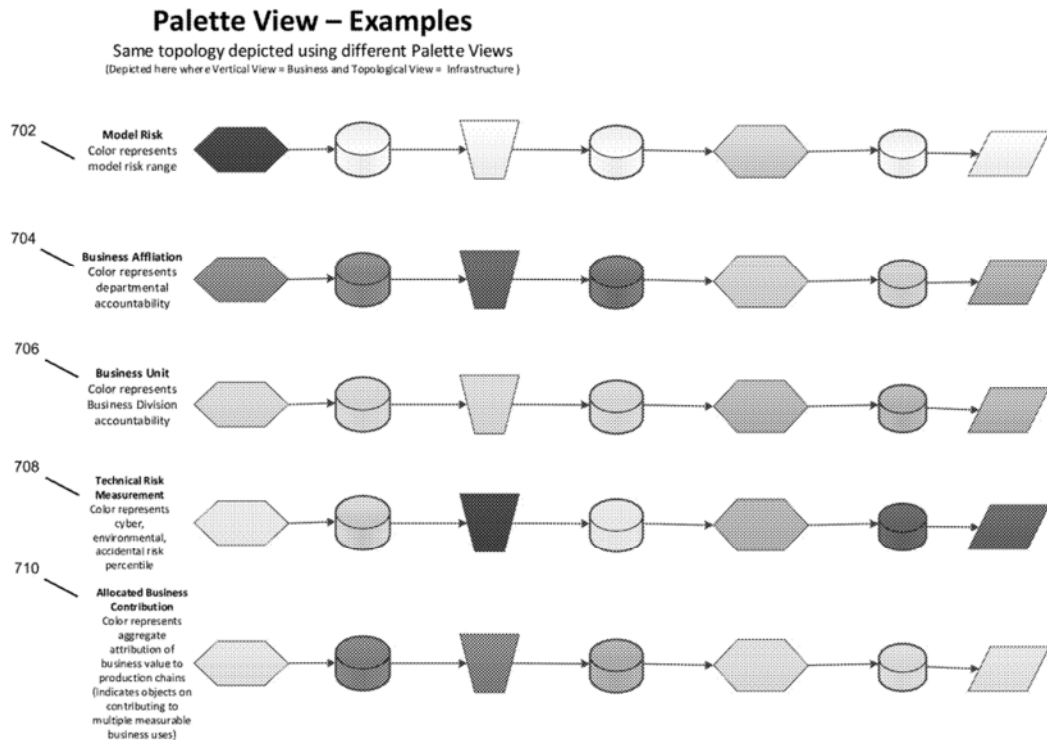


FIGURE 7

As shown in Fig. 16, a user may process and view objects in a variety of ways, called “Views,” including by threat vectors, which “fills the object shapes based on the value of the **technical risk** ranking characteristics of that object,” *id.*, 16:21-23, 14:7-15:10, Fig. 16. These Views may be combined—*e.g.*, “model risk” with “threat vector.” *Id.*, 14:7-9.

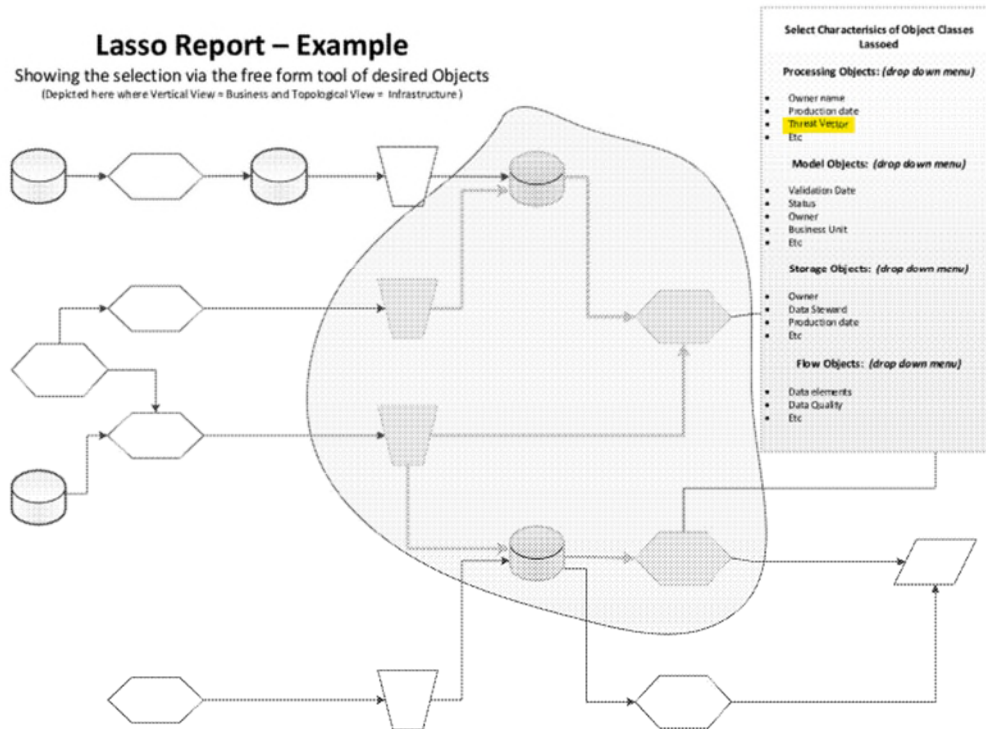


FIGURE 16

A POSITA would understand that Keenan discloses a threat modeling system and method. Keenan discloses “an Integrated Object Environment (IOE) running in a graph database environment,” which associates “risks” to assets (*i.e.*, sources of threats / threat model components)—*i.e.*, Keenan’s method and system includes identifying and measuring risk. *E.g.*, *id.*, Abstract; 1:31-46. A POSITA would understand that Keenan’s “risk” includes threats because measuring risk includes a determination of threats. *Id.*, 16:40-51; EX-1003, ¶79. And, as demonstrated, for example, by disclosures cited herein, 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. *E.g.*, EX-

1005, 1:37-45, 5:25-35 (“These security **risks** can be manually and/or automatically identified by **a threat modeling module.**”); EX-1007, 1:52-58; EX-1003, ¶79; EX-2011, p.94. The ’366 patent also recognizes that threat modeling is used in risk analysis. EX-1001, 2:3-20, 2:45-46, 14:5-17, 15:26-45, 15:64-16:3, 17:60-64, 18:9-12, 22:13-27, 22:28-37, 23:7-12, 23:42-48, 24:53-61, 25:7-12, 25:20-29, 26:38-45, 26:50-58, 32:59-62, 34:31-39, 35:35, 35:50, 39:47-54. Keenan discloses a method and system of measuring risk through threat modeling by providing “visual depictions” of the risk, *i.e.*, through visually depicting threats against IOE objects and creating “Views” through threat vectors, which may be combined with other Views, such as “model risk.” *Id.*, 14:7-15:10; *see also id.*, Abstract, 4:46-51, 4:64-67, 9:42-47, 18:6-14, Figs. 1, 7, 16. Based on these disclosures, a POSITA would understand that Keenan discloses a threat modeling system and method. EX-1003, ¶¶78-79.

b. Element 1[a]. “providing one or more databases, the one or more databases comprising:”

Keenan discloses this element. EX-1003, ¶80. Keenan discloses that the risk, risk characteristics, models, threat vectors, graphical views, imported Visio diagrams, and everything else in the disclosed IOE system is stored in the “**topology graph database.**” *Id.*, 5:37-44; *see also* Abstract, 5:45-62, Figs. 1, 4.

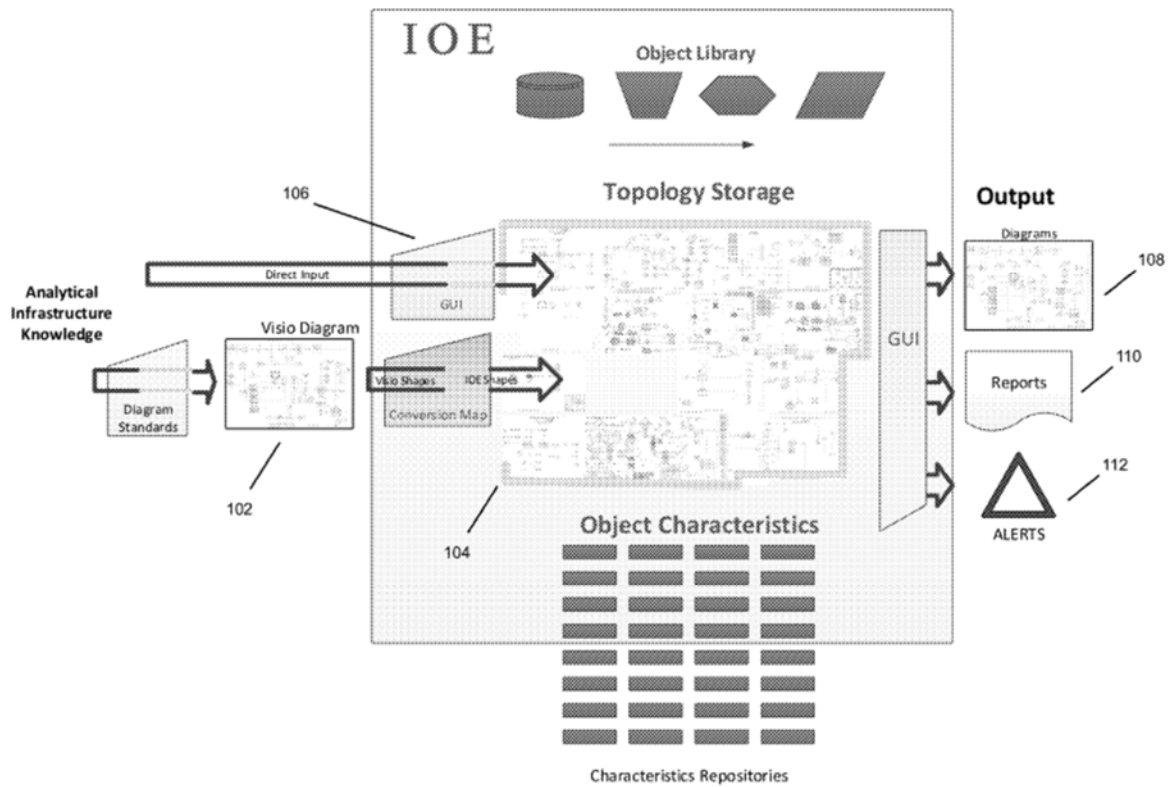


FIGURE 1

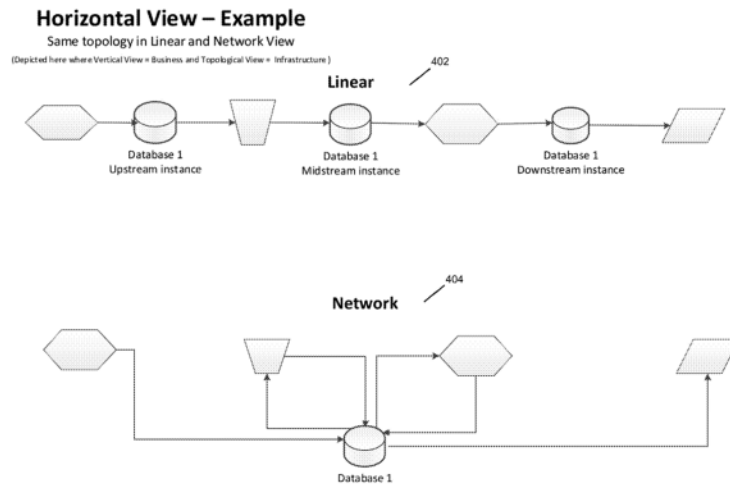


FIGURE 4

- c. **Element 1[b]. “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;”

Keenan teaches this element. EX-1003, ¶¶81-83. Keenan discloses “a plurality of threat model components” and “a plurality of threats” “wherein each of the threats is associated with at least one of the threat model components” because Keenan teaches an IOE that represents “a dynamic map of an enterprise’s analytic infrastructure, preferably including *all physical assets* that contribute to the analysis.” EX-1004, 5:27-44. Each asset or “real world component,” *i.e.*, physical asset, is defined by an object within the IOE and is associated with risk and characteristics (*e.g.*, risk characteristics and the relationship to other objects). *Id.* The IOE allows a user to select views that display the associated risk and consequences for specific assets using threat vectors and models. *Id.*, 4:64-67, 16:1-29; *see also* 1:31-52, 7:41-59, 13:4-22, 14:35-39, 14:61-63, 16:40-63, 17:32-40, 18:6-22, 20:34-51, Figs. 1, 7. Keenan further explains that certain Views use color to “represent different types of risk (*e.g.*, cyber, environmental, accidental, etc.).” *Id.*, 16:40-51.

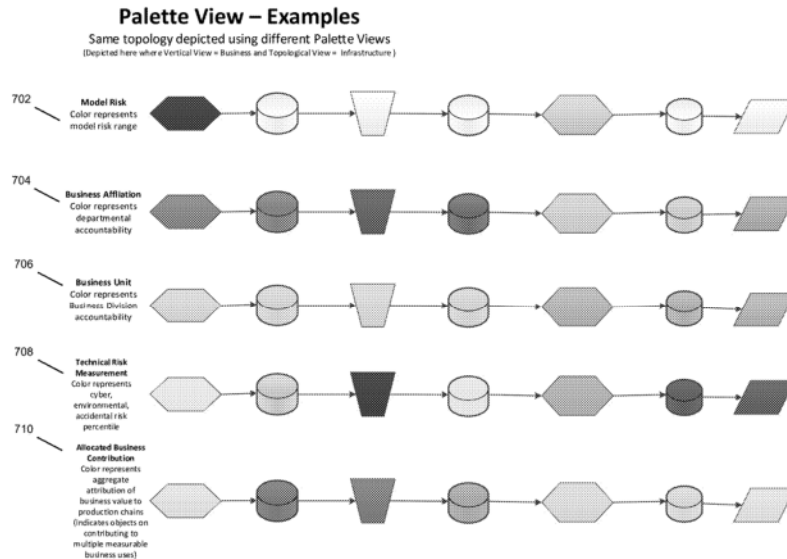


FIGURE 7

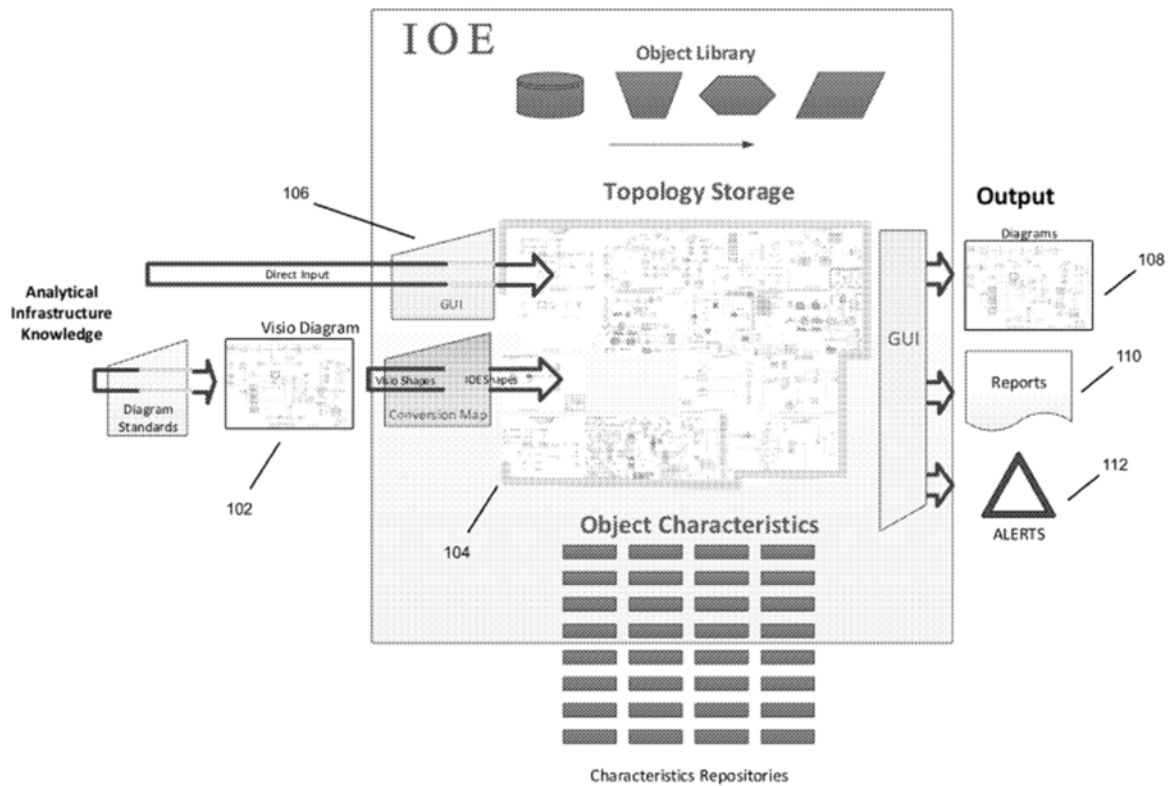


FIGURE 1

A POSITA would understand that the assets/objects in Keenan are “relevant sources of threats” and thus threat model components, as defined by the ’366 patent, because the assets/objects in Keenan are subject to risks that Keenan’s system measures. EX-1003, ¶82. A POSITA would further understand that Keenan’s “risk” includes threats because measuring risk includes a determination of threats, and Keenan discloses that Views may use color to “represent different types of risk (e.g., cyber, environmental, accidental, etc.).” *Id.*, 16:40-51; EX-1003, ¶82. The “types of risk” are threats because the described examples are threats (cyber/environmental/accidental). Thus, Keenan discloses threats within its risk analysis. A POSITA would further understand that “each of the threats is associated with at least one of the threat model components” because Keenan discloses associating risk with each asset. *Id.*, 1:33-38; *see also* 1:47-52; Element 1[p]; EX-1003, ¶82.

A POSITA would further understand that Keenan’s threats and threat model components are “stored therein” in the database, and that the threats and threat model components are associated “through the one or more databases” because Keenan discloses a method and system that is run in a “graph database environment.” *See* Element 1[a]; EX-1003, ¶83.

d. Element 1[c]. “providing one or more mapping files communicatively coupled with the one or more databases,”

Keenan discloses this element. EX-1003, ¶¶84-86. Keenan teaches a preset “map” that “*maps Visio shapes and formats to IOE shapes and formats,*” as well as diagrams and “Views” on a Graphical User Interface. EX-1004, 18:36-40, *see also* 16:5-11, 5:27-44 (“The IOE...represents a dynamic map”), 11:65-12:4, 12:11-62, 16:5-11, 18:23-28, Fig. 7.

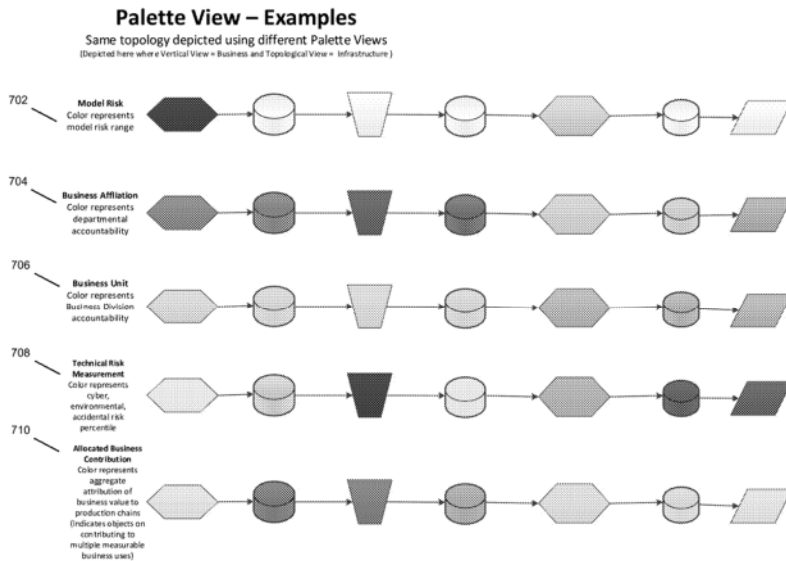


FIGURE 7

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. EX-1003, ¶85.

A POSITA would further understand that Keenan’s mapping file is “communicatively coupled with the one or more databases” because Keenan

discloses software that “converts the **graph database** and associated characteristics into Views.” See Element 1[a]; EX-1003, ¶86.

- e. **Element 1[d]. “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”); and”**

Keenan discloses this element. EX-1003, ¶¶87-88. Keenan teaches that a user may import Visio shapes and formats, where the system then “**maps Visio shapes and formats to IOE shapes and formats.**” *Id.*, 18:36-50. The IOE shapes and formats (*i.e.*, objects/assets) are threat model components. Element 1[b]. Thus, Keenan discloses “mapping,” *i.e.*, through one or more mapping files, Keenan’s threat model components with **Visio** shapes and formats. A POSITA would understand that the Visio shapes and formats in Keenan are “visual diagram components” because a user the Visio shapes and formats are “mapped,” *i.e.*, visually associated, with objects, which Keenan’s system visualizes, and because “shapes and formats” are tools used for visualization. *Id.*, 18:6-40; see also *id.*, 5:27-44, 18:23-50, 19:17-29, 21:10-17, Figs. 12-13; EX-1003, ¶87.

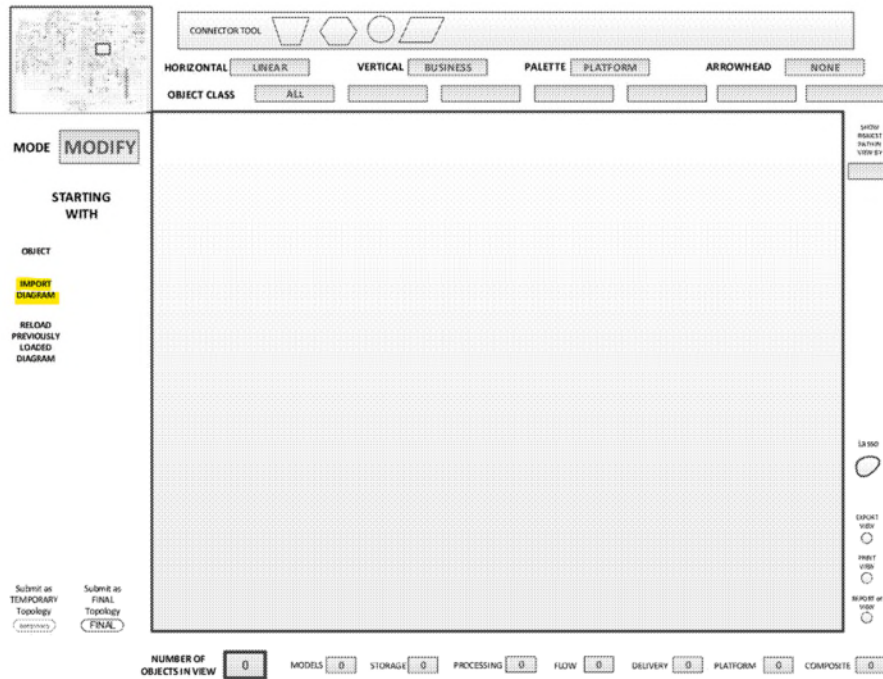


FIGURE 12

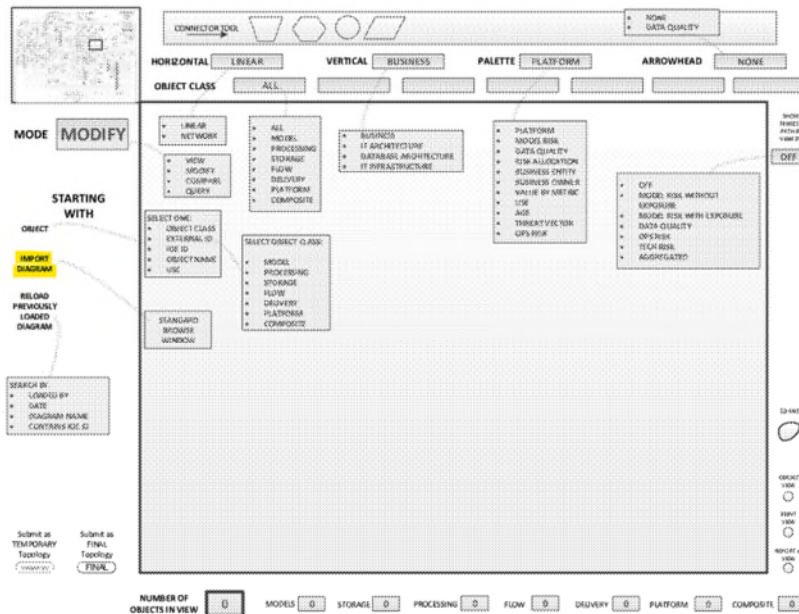


FIGURE 13

A POSITA would further understand that the Visio shapes and formats are “of a third party software application” because user of Keenan’s system selects the

option to “**import**” the Visio visual diagram components to Keenan’s system. *Id.*, 18:36-40. Further, Keenan teaches a method and system that “**converts**” Visio files “into a standard, canonical format for storage.” *Id.*, 5:37-44. Moreover, a POSITA viewing Keenan would understand that Visio is an independently-created software application “not created with a common schema, ***such that a mapping file or the like as claimed in the claims would be useful to map between the two software application,***” as defined in the file history, because Keenan utilizes a mapping file to map between the elements of Visio and Keenan’s system. *Id.*, 18:36-40; EX-1003, ¶88.

f. Element 1[e]. “in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:”

Keenan discloses this element. EX-1003, ¶¶89-91. Keenan teaches “in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices” because Keenan discloses that “[i]n embodiments of the present system, there are preferably four modes ***for the user to interact with the IOE via a Graphical User Interface (GUI)***,” EX-1004 at 11:42-43, 18:6-11, which are “implemented by relevant computing hardware instructed by a program,” *id.*, 21:26-33. Figs. 2 and 3 show “an exemplary GUI”:

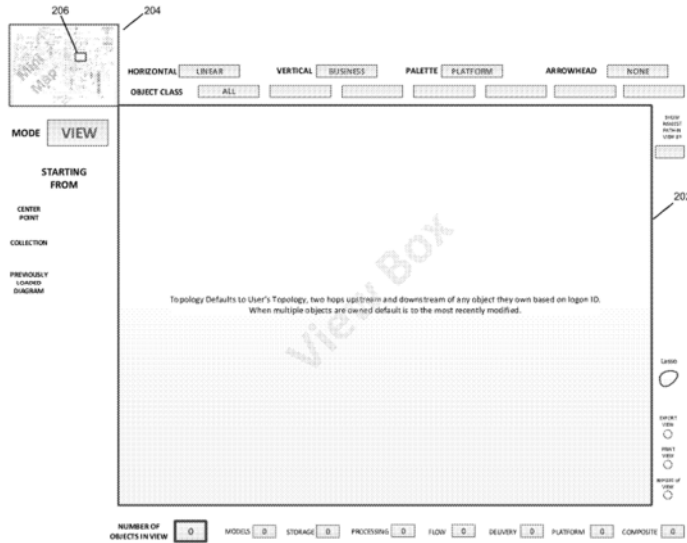


FIGURE 2

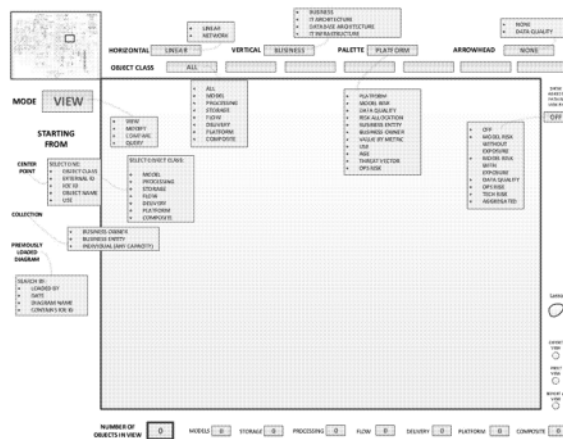


FIGURE 3

See also, e.g., *id.*, Abstract, 1:53-60, 2:3-6, 4:5-14, 5:24-27, 5:40-44, 11:42-64, 12:64-14:10, 18:36-50, Figs. 4-16.

A POSITA would understand that the user interface and the computing device are “communicatively coupled with the one or more databases” because Keenan discloses that the GUI and computing device are used to interact with the

IOE—and the IOE runs on a graph database which is then implemented by the computing device. *See id.*; Element 1[a]; EX-1003, ¶91.

- g. **Element 1[f]. “using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”**

Keenan discloses this element. EX-1003, ¶¶92-96. Keenan teaches “reading a data file generated by the third party software application” because Keenan discloses a system that “*maps Visio shapes and formats to IOE shapes and formats.*” EX-1004, 18:36-40; Element 1[d]. A POSITA would understand that the data file must be “read,” for example, when imported and when Keenan’s system “converts the Visio files 102 into a standard, canonical format.” EX-1004, 5:27-44; EX-1003, ¶92.

Keenan further discloses that “the data file comprising a subset of the third party diagram components.” *See* Element 1[d].

Keenan further discloses “the data file defining one or more relationships between the subset of third party diagram components” because Keenan discloses that “each real world component in the infrastructure is defined as an object with associated characteristics such as...*its relationship to other objects,*” where the objects are “*stored in a graphical format 102 such as a Visio file.*” EX-1004, 5:33-40. Keenan’s system imports and “converts the Visio files 102 into a

standard, canonical format,” and then defines the relationships between the subset of third party diagram components. *Id.*; *see also id.*, 1:24-30, 4:39-45, 4:54-60, 5:51-62, 7:25-34, 8:21-41, 15:15-43; EX-1003, ¶¶94.

Keenan further discloses that the data file is read in response to user inputs because Keenan discloses that the user imports Visio diagrams, which are then converted into a standard format. *Id.*, 5:33-40, 18:36-40; Element 1[d]; EX-1003, ¶¶95.

A POSITA would understand that this element is performed “using one or more computing devices.” *See* Element 1[e]; EX-1003, ¶¶96.

h. 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;”

Keenan discloses this element. EX-1003, ¶¶97-100. Keenan teaches “determining ... for the subset of third party diagram components, correlated threat model components as defined in the one or more mapping files” because Keenan discloses that a “map is preset that maps Visio shapes and formats to IOE shapes and formats. ... The existing ***Objects are then updated with new relationships based on the imported Visio diagram.***” EX-1004, 18:36-50; *see also id.*, 5:27-44, 18:23-50, 19:17-29, 21:10-17; Element 1[c]-1[d]. A POSITA would understand that Keenan’s disclosure describes “determining” the claimed relationships of

which threat model components are correlated with the third party diagram components in the mapping file because “existing objects are updated with new relationships” based on the importation of Visio diagrams—*i.e.*, the system must determine the relationships before updating new relationships. EX-1003, ¶¶97-98.

Keenan further discloses this limitation is performed in response to user inputs because Keenan discloses that “[t]he user selects the import function in the IOE GUI” to bring in Visio shapes and formats. *Id.*, 18:36-40. Keenan’s system then determines, for the subset of third party diagram components (*i.e.*, Visio shapes and formats) correlated threat model components (*i.e.*, assets/objects). See Elements 1[b], 1[d], 1[e]; EX-1003, ¶99.

A POSITA would understand that this element is performed “using one or more computing devices.” See Element 1[e]; EX-1003, ¶100.

- i. **Element 1[h]. “displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”**

Keenan discloses this element. EX-1003, ¶¶101-105. Keenan teaches “a relational diagram” because Keenan discloses an IOE including “*diagrams*” that “*link[] together*” “information assets” in the IOE. EX-1004, 1:24-30. These diagrams are displayed on the GUI and “serve[] as a communication medium to

and from users and the IOE,” *id.*, 2:5-6, showing the “[r]epresentation of **the relationships between objects**” in the IOE, *id.*, 5:5-10, and are thus “relational diagrams” as claimed. A POSITA would understand that the interface displays a relational diagrams include “one of a system, an application, and a process” because Keenan discloses these relationships in the relational diagram “represent the **storage, processing and flow of information**,” *id.*, 5:5-10, as well as other diagrams or “Views” (which Keenan notes is synonymous with diagrams, *id.*, 5:24-27) showing systems, applications, and processes, *id.*, 1:24-33, 2:5-17, 4:5-14, 4:46-60, 5:5-10, 5:17-19 (topology “[d]epicts tasks in process order **sequence**”); 7:60-62 (“Platform Objects include physical and/or software **systems** that house...models”), 9:56-63, 10:37-50, 11:42-64, 18:66-19:5 (“The **icon** [in the GUI] represents the document format. **By clicking on this icon, the application** which supports the document opens and the document appears on the screen.”), Figs. 1-3, 9, 12-15. Moreover, a POSITA would understand that the IOE GUI display as a whole with the imported Visio diagram components represents, as shown in the Figures, *e.g.*, Figs. 1 and 10, are “one of a system, an application, and a process.”

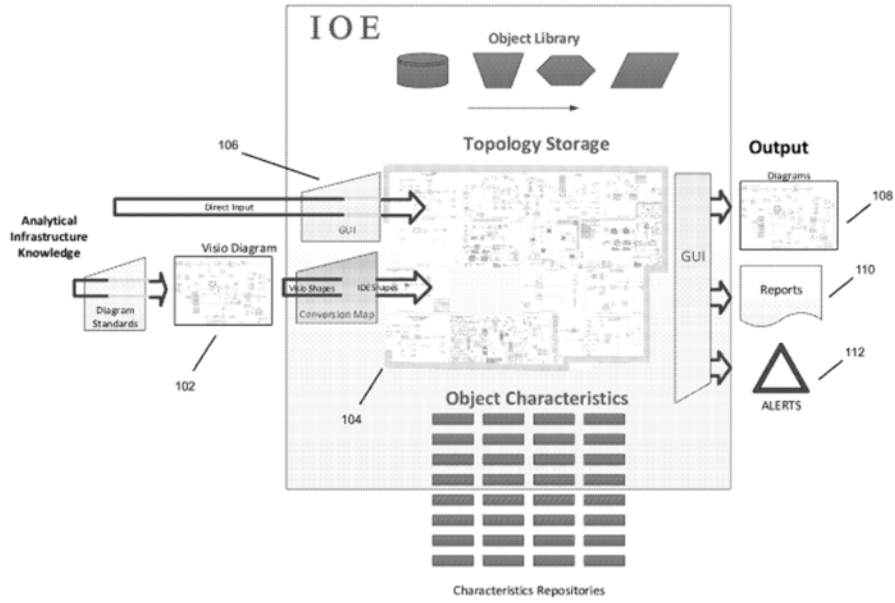


FIGURE 1

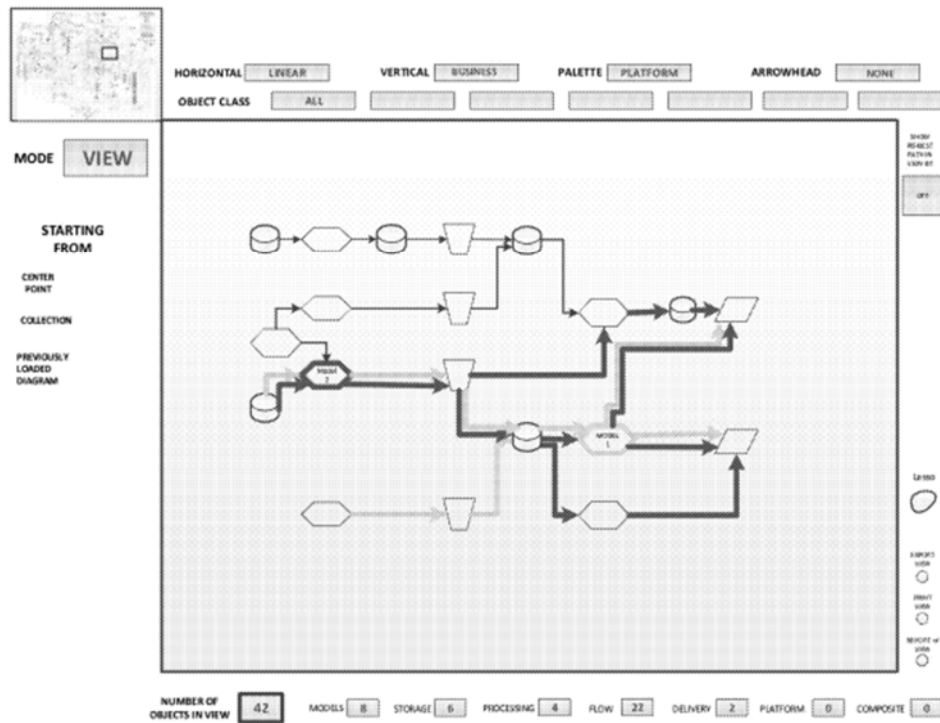


FIGURE 10

A POSITA would further understand that this relational diagram is displayed on the one or more interfaces “using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model” because Keenan discloses that “existing Objects are [] updated with new relationships based on the imported Visio diagram”—*i.e.*, imported Visio diagrams associated with objects, *see* Element 1[d], are updated to “represent the ***storage, processing and flow of information,***” and/or other systems and processes cited above. EX-1003, ¶102.

Keenan further discloses “the relational diagram defining a threat model.” *See* Element 1[p].

Keenan further discloses this limitation is performed in response to user inputs because Keenan discloses that “[t]he user selects the import function in the IOE GUI” to bring in Visio shapes and formats. *Id.*, 18:36-40. Keenan’s system then determines, for the subset of third party diagram components (*i.e.*, Visio shapes and formats) correlated threat model components (*i.e.*, assets/objects) and associated visual representations. *See* Elements 1[b], 1[d], 1[e].

Keenan further discloses that the display is on “one or more user interfaces.” *See* Element 1[e]; EX-1004, 2:3-6; EX-1003, ¶105.

- j. **Element 1[i]. “generating, using the one or more computing devices, and displaying, on the one or more user interfaces, 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 discloses this element. EX-1003, ¶¶106-108. Keenan teaches a reporting system that converts user inputs into “Views,” which are “exportable as *reports*.” EX-1004, 5:40-44; *see also id.*, 8:15-20, 17:11-40, 18:6-22, 19:30-65, Figs. 1, 3, 5, 11-15, 16. 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. *Id.*, 17:38-40, Fig. 16.

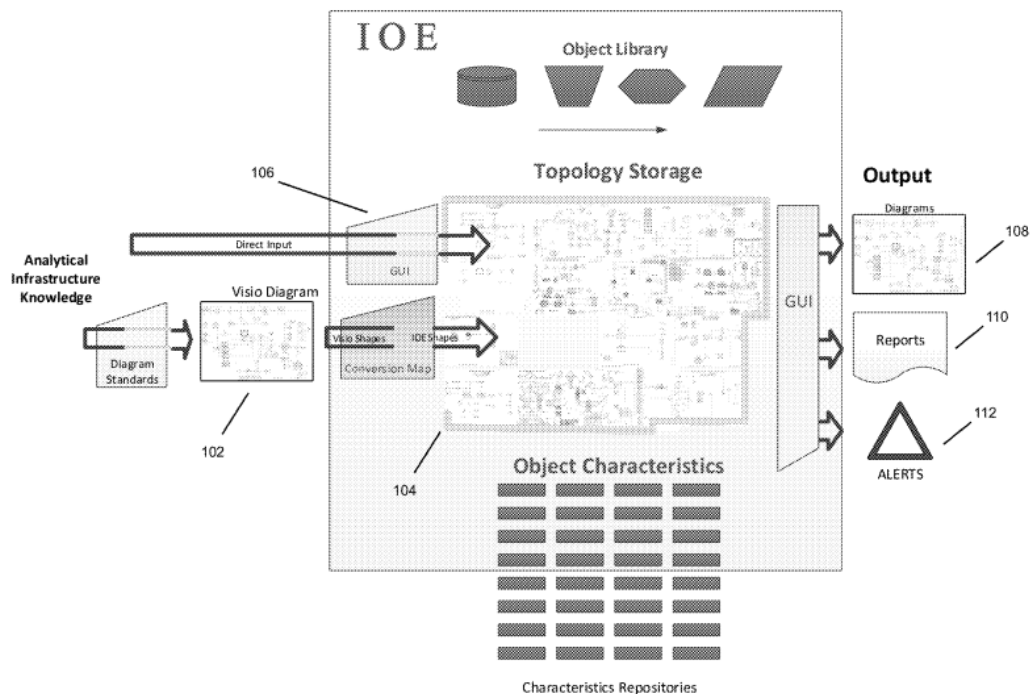


FIGURE 1

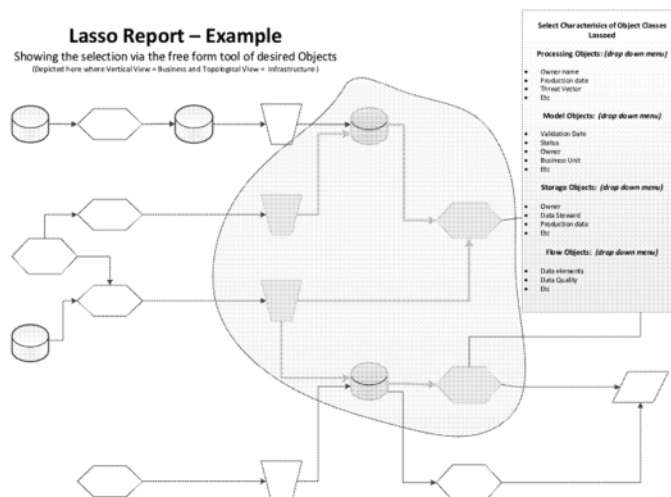


FIGURE 16

Keenan further discloses this limitation is performed in response to user inputs because Keenan provides software that its Views “are **exportable** as ... as **reports.**” *Id.*, 5:40-44. A POSITA would understand “exportable” to mean “the ability for a user to export” in context. EX-1003, ¶107.

A POSITA would understand that this element is performed “using one or more computing devices.” See Element 1[e]; EX-1003, ¶108.

2. Claim 2: “The method of claim 1, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”

Keenan discloses this element. EX-1003, ¶109. Keenan teaches that its system and method may be “implemented by relevant computing hardware instructed by a program. **The program may be stored in a computer readable storage medium,**” which may be “**a ROM, a RAM, a magnetic disk or a compact disk.**” EX-1004, 21:27-33. A POSITA would understand that Keenan discloses

this element because although Keenan discloses storage through a graph database, but further provides that programs implementing the IOE, such as the Visio mapping files, may be stored on a computer readable medium, including ROM or RAM. EX-1003, ¶109. Computer readable storage mediums are mediums capable of storing data in a format readable by a mechanical device, and a POSITA would understand that Keenan’s reference to ROM or RAM indicates that files are stored on a computing device because ROM and RAM are both forms of computer storage. *Id.*

3. Claim 3: The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.

Keenan discloses this element. EX-1003, ¶110. Keenan teaches “[t]o connect objects on the screen, the GUI provides Flow Objects, which preferably connect to any point on the Object shape in the diagram to allow for clarity in the depiction of the topology. Double clicking on the object *opens the characteristics table.*” EX-1004, 18:65-19:2; *see also id.*, 8:16-20, 13:53-55,

4. Claim 4: “The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file.”

Keenan discloses this element. EX-1003, ¶111. As discussed, Keenan discloses a data file that comprises Visio shapes and formats. *See* Element 1[f]. A

POSITA would understand that Visio files can be a “VSD file” or a “VSDX file.”

EX-1003, ¶111.

5. **Claim 5: “The method of claim 1, wherein determining, for the subset of third party diagram components, correlated threat model components, comprises first determining whether a user-defined name for one of the subset of third party diagram components has a match in the one or more mapping files and, if no match is found, then determining whether a default title for the third party diagram component, as defined by the third party software application, has a match in the one or more mapping files.”**

Keenan discloses this element. EX-1003, ¶¶112-113. Keenan teaches that “[e]ach object preferably has two identifiers: *one internal to the IOE*, and one that ties the object to an authoritative *external* repository. ... Therefore, all ‘model’ objects in the IOE preferably carry their repository IDs as well as an ID internal to the IOE.” EX-1004, 6:13-26. Keenan further teaches that “[a] map is preset that maps Visio shapes and formats to IOE shapes and formats. The user selects the import function in the IOE GUI, *which first checks to see if object already exists in IOE based on external ID number first, then name match.*” EX-1004, at 18:36-50. A POSITA viewing Keenan would understand that an “external ID” is a default title as claimed and a “name match” or “Name of object” is a user-defined name.

Moreover, a POSITA would further understand that Keenan discloses a system that checks for default titles or user-defined name matches in either order

because Keenan's system allows a user to "select a method for **adding an object**, such as External Object ID ... and Name of object." *Id.*, 18:51-60. The IOE then "returns a topology a topology with the object(s) already stored **that match the criteria the user entered**, then the user can browse the list to see if the object they want to load is already in the IOE. If not, the user can then add the object." *Id.*; see also *id.*, Fig. 13; EX-1003, ¶113.

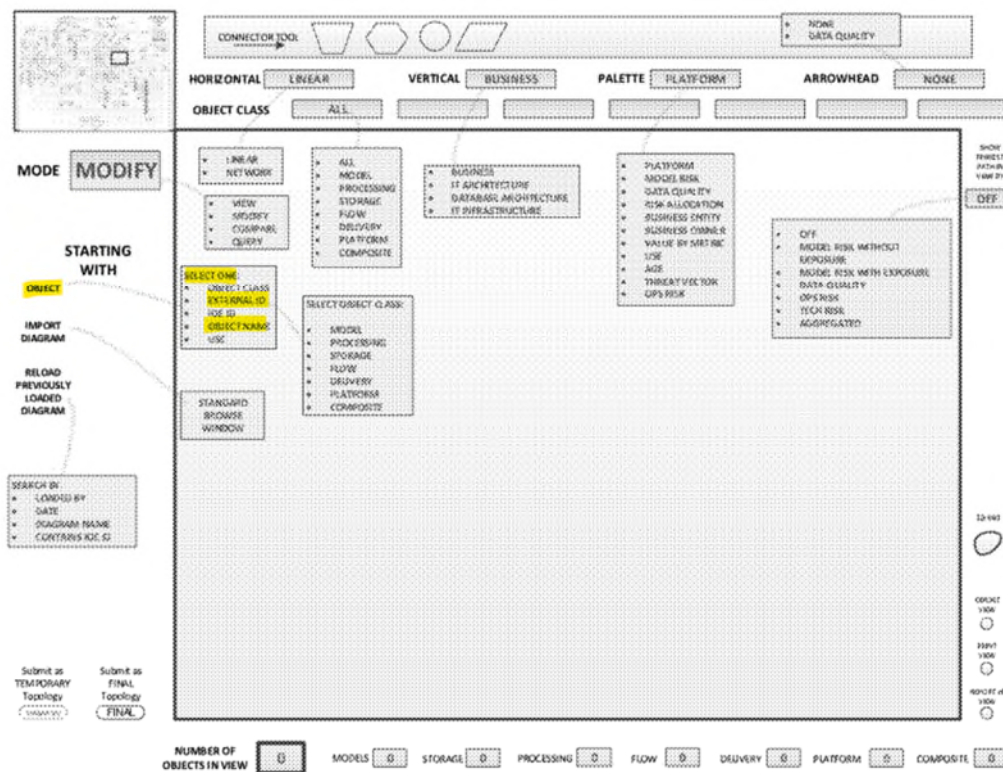


FIGURE 13

6. **Claim 6: "The method of claim 5, further comprising, if no match is found for the default title, matching the third party diagram component with a placeholder component and**

displaying the placeholder component on the relational diagram to indicate that no match was found.”

Keenan discloses this element. EX-1003, ¶¶114-116. Keenan discloses that “[t]he user selects the import function in the IOE GUI, which first checks to see if object already exists in IOE based on external ID number first, then name match. ***If the object already exists***, a message is posted to the screen, such as, ‘The following objects matched existing objects from the IOE, new relationships will be loaded to existing object.’” EX-1004, 18:36-50. If the object a user wants is not in the IOE, however, ***“the user can then add the object.”*** *Id.*, 18:51-60. A POSITA would understand that Keenan’s system creates a placeholder component where no exact match is found for the third party component object the user adds to Keenan’s IOE, and then displays that placeholder in the IOE, indicating no match was found. The user then may select the object to provide an “Object Name to identify an object,” so that the object is now part of the IOE and no longer a placeholder. *Id.*, 13:53-65; EX-1003, ¶114.

Moreover, Keenan discloses the option to submit “temporary” topology objects in memory that are displayed on the GUI, as shown in Figs. 12 and 13:

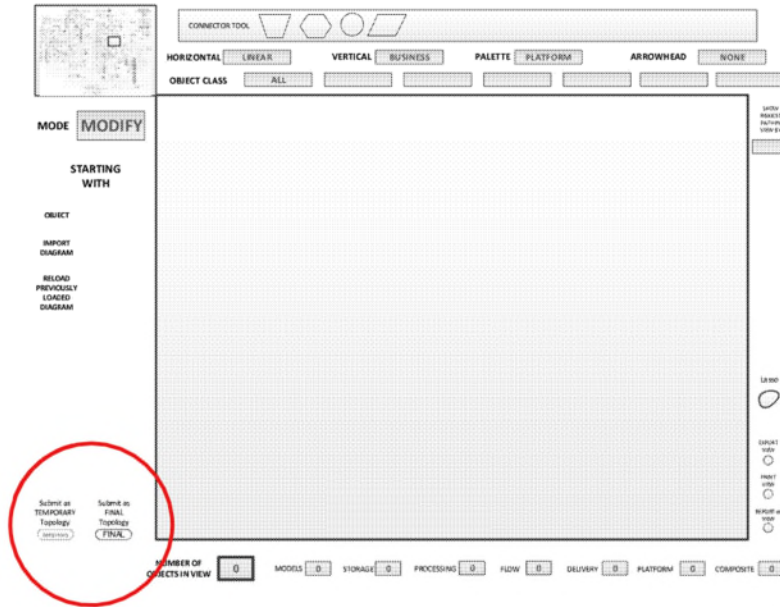


FIGURE 12

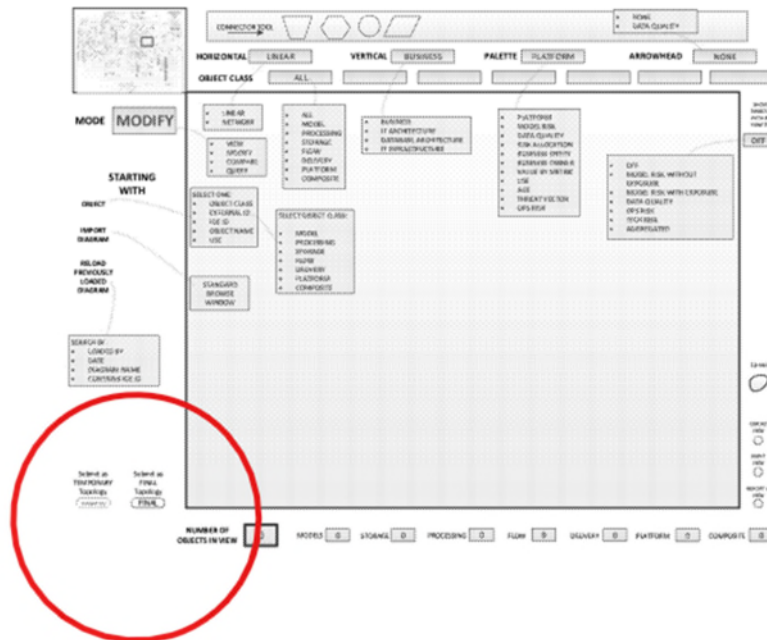


FIGURE 13

See also EX-1004, 11:7-11, 19:9-16. A POSITA would understand that these temporary placeholder components are used where no match is found for the default title, and Keenan's system may match the third party diagram component Visio shapes and formats with a "temporary" placeholder component object and

display that placeholder component on the relational diagram to indicate that no match was found. EX-1003, ¶116.

7. **Claim 7: “The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files.”**

Keenan discloses this element. EX-1003, ¶¶117-118. As discussed in Element 1[f], Keenan discloses “the data file defining one or more relationships between the subset of third party diagram components” because Keenan discloses that “each real world component in the infrastructure is defined as an object with associated characteristics such as state, *and its relationship to other objects*. The objects and characteristics *are stored in a graphical format 102 such as a Visio file*. The system converts the Visio files 102 into a standard, canonical format for storage in a topology graph database.” EX-1004, 5:33-40. Keenan’s system further includes “data flow objects” that represent the relationships between objects. *Id.*, 1:24-30, 4:39-45, 4:54-60, 5:51-62, 7:25-34, 8:21-41, 15:15-43. A POSITA would understand that these data flow objects represent, among other things, the one or more relationships defined by the data file. EX-1003, ¶117.

Keenan’s system further provides “a method by which *data flow objects could be separately linked to the components*.” A POSITA would understand this disclosure to mean that the data flow objects, *i.e.*, the one or more relationships

defined by the data file, may be correlated with the threat model components, *i.e.*, assets/objects, independently. EX-1003, ¶118.

8. Claim 8:

- a. Element 8[p]. “A threat modeling system, comprising: one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:”**

Keenan discloses this element. EX-1003, ¶119. A POSITA would understand that Keenan’s one or more databases is communicatively coupled with one or more computing devices because Keenan discloses that its method and system is “implemented by relevant computing hardware instructed by a program.” *Id.*, 21:26-33; Elements 1[p]-1[a] and 1[e]; EX-1003, ¶119.

- b. Element 8[a]. “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;”**

Keenan discloses this element. *See* Elements 1[b].

- c. Element 8[b]. “one or more mapping files communicatively coupled with the one or more databases, 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 discloses this element. *See* Elements 1[c]-1[d].

- d. Element 8[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user**

input, initiate reading of a data file by one of the one or more computing devices, the data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”

Keenan discloses this element. EX-1003, ¶¶122-123; Elements 1[e]-[f]. As shown in Figs. 12-13, Keenan discloses “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by one of the one or more computing devices” because Keenan discloses that “*[t]he user selects the import function in the IOE GUI, ... The existing Objects are then updated with new relationships based on the imported Visio diagram.*” EX-1004, 18:36-50; see also 18:6-35; 5:27-44, 18:23-50, 19:17-29, 21:10-17, Figs. 12-13.

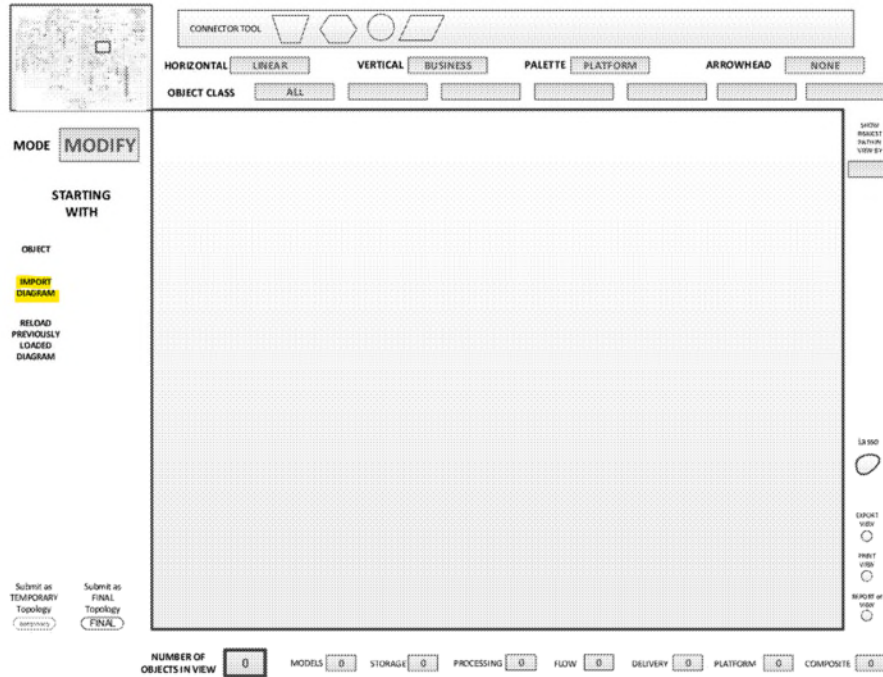


FIGURE 12

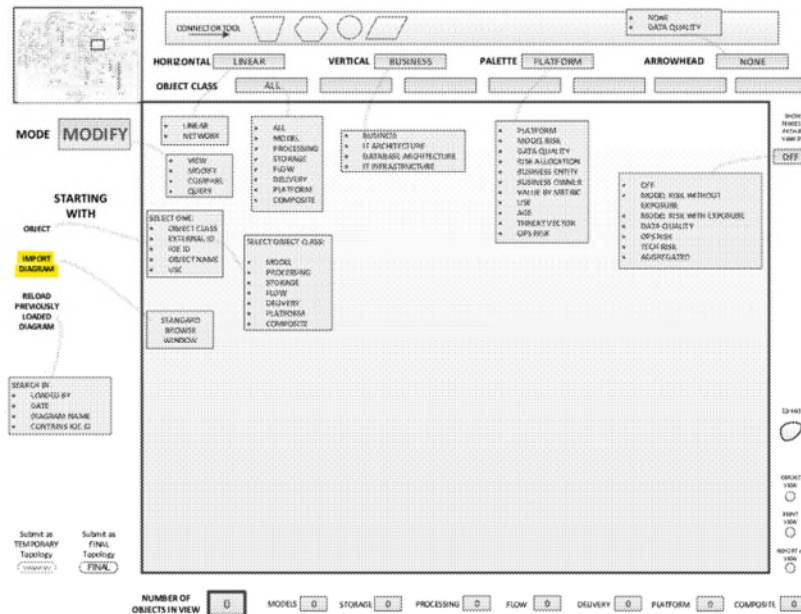


FIGURE 13

A POSITA would understand “the import function in the IOE GUI” to be an import interface displayed on a computing device as claimed because it allows a

user to import third party diagram components, *e.g.*, Visio shapes and formats, which are included in a data file. EX-1003, ¶123. A POSITA would further understand that Keenan’s import interface initiates reading of the data file because Keenan’s system checks for existing objects and forms new relationships after the user selects the import function. EX-1003, ¶123.

- e. **Element 8[d]. “an interface configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files;”**

Keenan discloses this element. *See* Element 1[g]; EX-1003, ¶¶124-125.

Keenan discloses “an interface” because Keenan allows a “***user to interact with the IOE via a Graphical User Interface (GUI)***,” such as by selecting the import function. EX-1004 at 11:42-43; *see* Elements 1[e], 8[c].

Keenan further teaches that the interface is “configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files” because Keenan teaches a “map is preset that maps Visio shapes and formats to IOE shapes and formats. ... The existing ***Objects are then updated with new relationships based on the imported Visio diagram.***” EX-1004, 18:36-50; *see also* Element 1[d]. The importation “initiate[s] a determination” of which threat model components are correlated with the third party diagram components in

the mapping file because “existing objects are updated with new relationships” based on the importation of Visio diagrams—*i.e.*, the system must determine the relationships before updating new relationships. EX-1003, ¶125.

- f. **Element 8[e]. “a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”**

Keenan discloses this element. *See* Element 1[h]; EX-1003, ¶¶126-127. A POSITA would understand that the Keenan’s disclosures discussed in Element 1[h] also disclose “a diagram interface” because Keenan discloses that “[d]iagrams are rendered by a front end/GUI of the IOE and are both input and output of the IOE. Diagrams ... serve[] as a communication medium to and from users and the IOE.” EX-1004, 2:3-6; *see also* Element 1[h].

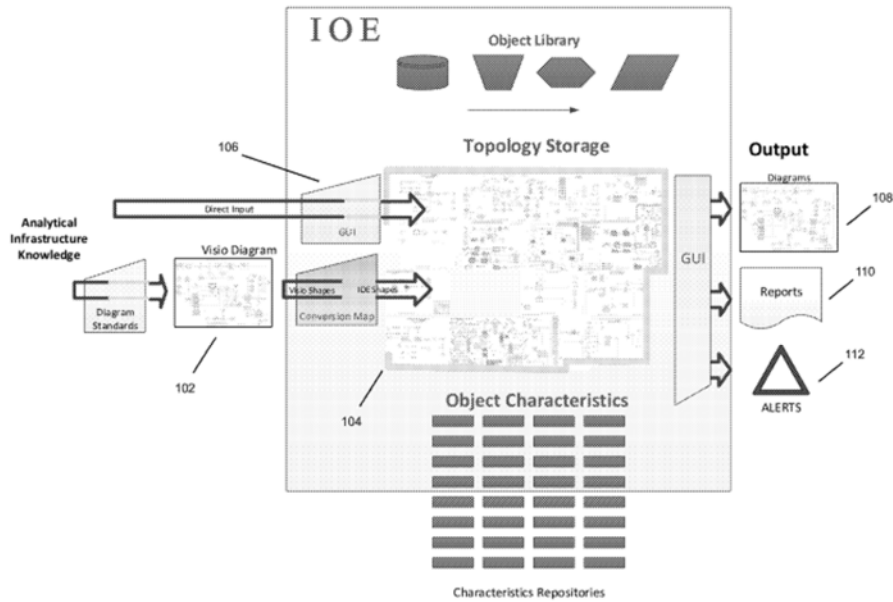


FIGURE 1

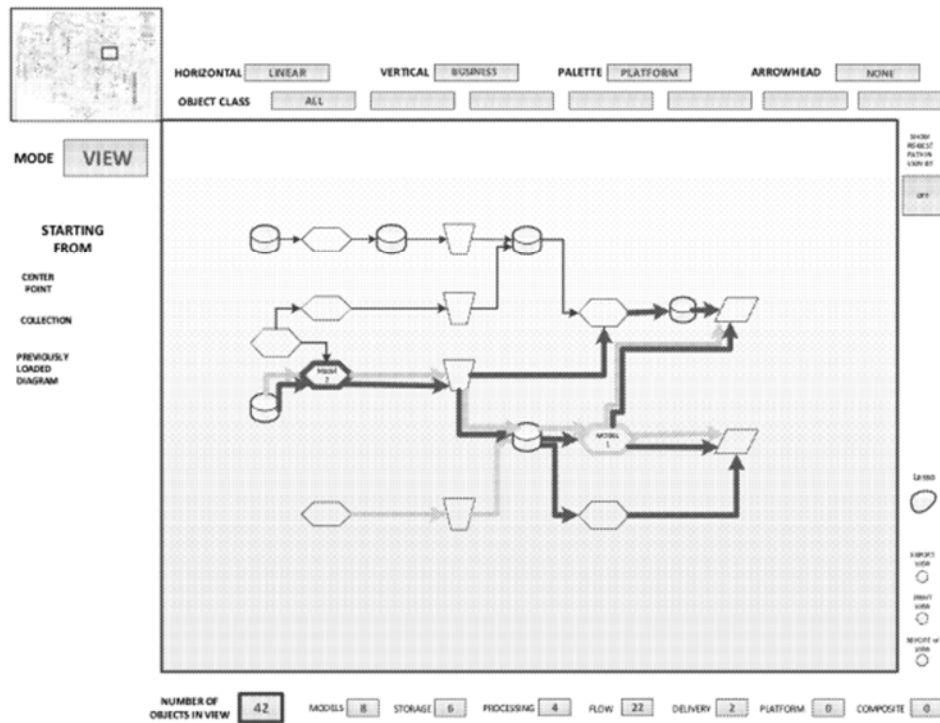


FIGURE 10

A POSITA would understand that this element is “displayed on the one or more computing devices.” See Element 1[e]; EX-1003, ¶127.

- g. Element 8[f]. “a threat report interface, displayed on the one or more computing devices, including 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 discloses this element. See Element 1[i]; EX-1003, ¶¶128-130. A POSITA would understand that the Keenan’s disclosures discussed in Element 1[i] also disclose “a threat report interface” because Keenan discloses Views that are “exportable,”—*i.e.*, interacted with through an interface, as reports. Views, which are exportable as diagrams 108, as well as **reports 110** and alerts 112.” EX-1004, 5:40-44.

A POSITA would understand that this element is “displayed on the one or more computing devices.” See Element 1[e]; EX-1003, ¶130.

- 9. Claim 9: “The system of claim 8, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”**

Keenan discloses this element. See Claim 2.

- 10. Claim 10: The system of claim 8, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.**

Keenan discloses this element. See Claim 3.

11. **Claim 11: “The system of claim 8, wherein the data file comprises one of a VSD file, a VSDX file, a TMT File, an XML file, a JSON file, a PNG file, and a JPEG file.”**

Keenan discloses this element. *See* Claim 4.

12. **Claim 12: “The system of claim 8, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components.”**

Keenan discloses this element. EX-1003, ¶¶134-135; *see also* Claim 5.

Keenan teaches that “[e]ach object preferably has two identifiers: ***one internal to the IOE***, and one that ties the object to an authoritative ***external*** repository. ...

Therefore, all ‘model’ objects in the IOE preferably carry their repository IDs as well as an ID internal to the IOE.” EX-1004, 6:12-26. A POSITA viewing Keenan would understand that an “external ID” is a default title as claimed and a “name match” or “Name of object” is a user-defined name.

Keenan further discloses that “[t]o add an objection 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***, ... ***Name of object***. If the IOE returns a topology with the object(s) already stored that match the criteria the user entered, then the user can browse the list to see if the object they want to load is already in the IOE. If not, the user can then add the object. Alternatively, the user can modify the object(s) found.” EX-1004, 18:51-60. A POSITA would understand that Keenan’s system allows for a user to add an object by correlating

user-defined names of the third party diagram components with the threat model components—*i.e.*, through “Name of object,” **or** correlating default titles of the third party diagram components with the threat model components—*i.e.*, through “External Object ID.” A POSITA would further understand that this correlation is through “a file” because files are required to perform computer functions such as correlations. EX-1003, ¶135.

13. Claim 13: “The system of claim 8, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.”

Keenan discloses this element. EX-1003, ¶136; Claim 12. A POSITA would understand that Keenan’s system allows for a user to add an object by correlating user-defined names of the third party diagram components with the threat model components—*i.e.*, through “Name of object,” **or** correlating default titles of the third party diagram components with the threat model components—*i.e.*, through “External Object ID.” A POSITA would further understand that this correlation is through “a file” because files are required to perform computer functions such as correlations. *Id.*

14. Claim 14: The system of claim 8, wherein, for each of the subset of third party diagram components for which no correlated threat model component is found in the one or more mapping files, the diagram interface displays a

placeholder component indicative of a match not being found.

Keenan discloses this element. *See* Claim 6.

- 15. Claim 15: The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files.**

Keenan discloses this element. EX-1003, ¶¶138-140. Keenan discloses “a Modify mode, where the user can add, change and delete Objects or Characteristics” in the Views of the GUI—thus modifying the mapping interface. *Id.*, 11:46-47; *see also id.*, Abstract, 4:1-2, 11:61-64, 18:29-35, 18:51-60, 19:7-16, 20:61-21:9, Figs. 12-13. A POSITA would understand that the mapping file is modified when the view is modified. EX-1003, ¶138. A POSITA would further understand that a mapping interface is configured to modify as claimed because Keenan discloses a mapping interface—*i.e.*, a preset map that “maps Visio shapes and formats to IOE shapes and formats.” *Id.*; EX-1004, 18:36-50.

Keenan further discloses mapping interface is configured to modify “in response to user inputs” because Keenan explicitly specifies that a user may make modifications. *Id.*, 11:46-47.

A POSITA would understand that this element is performed “using one or more computing devices.” *See* Element 1[e]; EX-1003, ¶140.

16. Claim 16:

- a. Element 16[p]. “A threat modeling system, comprising: one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:”**

Keenan discloses this element. See Elements 1[p]-1[a], 1[e], and 8[p].

- b. Element 16[a]. “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;”**

Keenan discloses this element. See Element 1[a] and 8[a].

- c. Element 16[b]. “one or more mapping files communicatively coupled with the one or more databases, 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 discloses this element. See Elements 1[c]-1[d] and 8[b].

- d. Element 16[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by the one or more computing devices, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”**

Keenan discloses this element. See Element 8[c].

- e. Element 16[d]. “an interface configured to, in response to receiving user input, initiate a determination of which threat model components are**

correlated with the subset of third party diagram components in the one or more mapping files;”

Keenan discloses this element. *See* Element 1[g] and 8[d].

- f. Element 16[e]. “a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of a computing network, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”**

Keenan discloses this element. *See* Element 1[h] and 8[e].

- g. Element 16[f]. “a threat report interface, displayed on the one or more computing devices, including 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 discloses this element. *See* Element 1[i] and 8[f].

- 17. Claim 17: “The system of claim 16, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”**

Keenan discloses this element. *See* Claim 2.

- 18. Claim 18: The system of claim 16, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.**

Keenan discloses this element. *See* Claim 3.

- 19. Claim 19: The system of claim 16, wherein the one or more mapping files includes a file correlating user-defined names**

of the third party diagram components with the threat model components.

Keenan discloses this element. *See* Claim 5.

20. Claim 20: “The system of claim 16, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.”

Keenan discloses this element. *See* Claim 13.

C. Ground 2: Zheng In View of Baker and Jones Renders Obvious Claims 1-4, 7-11, 15-18

Zheng in view of Baker and Jones (collectively, the “Combination”) renders claims 1-3, 7-11, and 15-18 obvious. All three disclose threat modeling software applications. Baker discloses importing diagrams from Microsoft Visio into a threat modeling software application, and Jones discloses generating threat model reports within a threat modeling software application. EX-1003, ¶152.

1. Claim 1

a. Element 1[p]. “A threat modeling method, comprising:”

To the extent the preamble is limiting, the Combination discloses this element. EX-1003, ¶153. Zheng discloses “a system *that can dynamically produce interactive and predictive threat models...*” EX-1005, 1:37-45; *see also id.*, Title, Abstract, 1:24-33, 2:1-18, 2:25-29, 2:36-49, 5:6-24, 6:13-26.

b. Element 1[a]. “providing one or more databases, the one or more databases comprising:”

The Combination discloses this element. EX-1003, ¶154. Zheng discloses “at least one *database* table is used to *store data* for *each layer* and *for each possible combination/interaction* of the layers.” EX-1005, 8:14-9:10, 9:40-44, 10:35-39, Fig. 3.

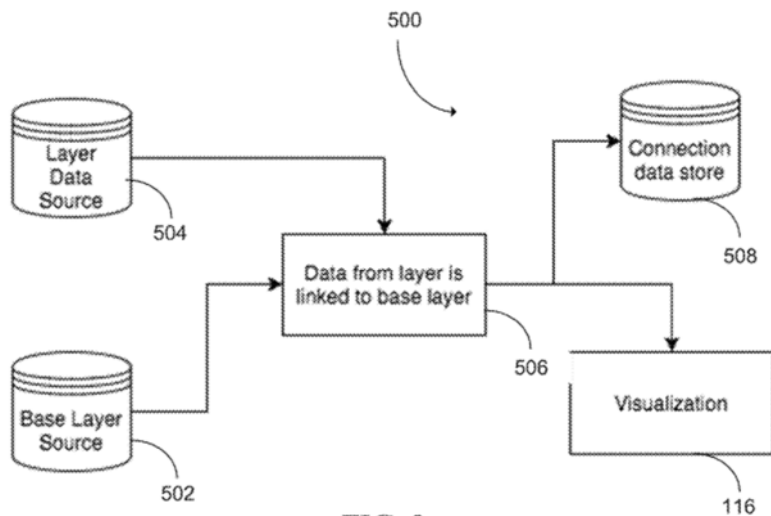


FIG. 3

c. Element 1[b]. “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;”

The Combination discloses this element. EX-1003, ¶¶155-159. Zheng discloses that “[e]ach threat can be visually associated with at least one of (i) *a threat actor application*, (ii) *a threat target application* and (iii) *a displayable vector connecting the two* to represent and visualize a particular attack

methodology.” EX-1005 at 5:14-18. Zheng’s “threat actor applications” are the claimed “plurality of threats,” and Zheng’s “threat target applications” are the claimed “plurality of threat model components” because, as in the claimed method, the system “***illustrate[s] the impact of the threat actor***” on the components of the base layer, such as the threat target applications. *Id.*, 12:1-3; *see also* 11:65-68. In other words, the threat target applications are relevant sources of threats (as defined by PO) impacted by the threats/threat actors. EX-1003, ¶157.

Zheng further discloses “wherein each of the threats is associated with at least one of the threat model components” because Zheng discloses that the threats (*i.e.*, threat actors) and threat model components (*i.e.*, threat targets) are “visually associated” via “a displayable vector” that connects the threats and threat model components. *Id.*; *see also id.*, 5:18-24 (“A threat can provide one-to-one ***mapping between a threat actor and a threat target.***”), 2:36-42.

These threat model components and threats are “stored” in and “associated ... through the one or more databases” because, as discussed in Element 1[a], Zheng discloses “at least one ***database*** table is used to ***store data*** for ***each layer*** and ***for each possible combination/interaction*** of the layers.” EX-1005, 8:25-27; Element 1[a]; EX-1003, ¶159.

d. Element 1[c]. “providing one or more mapping files communicatively coupled with the one or more databases,”

The Combination discloses this element. EX-1003, ¶¶160-163. Zheng discloses that “**visualization**” of “a company's application architecture” and “**threat detection based on the visualization.**” Zheng accomplishes visualization through “**mapping techniques and concepts...in the context of data visualization to create a graphical representation of application connectivity and security.**” EX-1005, 3: 24-34; *see also id.* 2:36-42, 5:18-24 (“**A threat can provide one-to-one mapping between a threat actor and a threat target.**”), 4:2-5, 3:49-53, 4:31-35, 11:10-13.

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. EX-1003, ¶162.

A POSITA would further understand that the one or more mapping files in Zheng are communicatively coupled with the one or more databases because Zheng discloses “at least one **database** table is used to **store data** for **each layer** and **for each possible combination/interaction** of the layers.” EX-1005, 8:25-27; EX-1003, ¶163; Element 1[a].

e. Element 1[d]. “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”); and”

The Combination discloses this element. EX-1003, ¶¶164-166. Baker discloses “visual diagram components of a third party software application” because Baker discloses that “risk management or control *flowcharts may be imported at step 104 from third party software such as that marketed as Microsoft Office Visio®.*” EX-1006, ¶[0025]; *see also id.*, ¶¶[0009], [0023], Fig. 4.

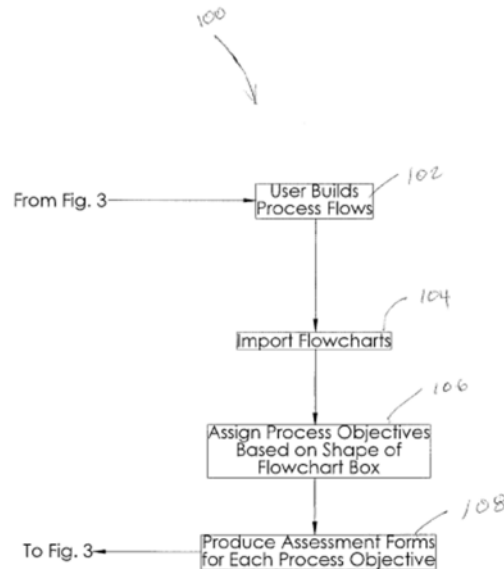


Fig. 4

A POSITA would understand that the Visio flowcharts are “of a third party software application” because Baker allows a user to select the option to “*import*” the Visio visual diagram components to Baker’s system, such that “a mapping file or the like as claimed in the claims,” such as the mapping file of Zheng, “would be

useful to map between elements of the two software applications,” as defined in the file history. *E.g.*, EX-1004, ¶[0023]; EX-1003, ¶164.

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 that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams. EX-1003, ¶166. Motivation for this combination is provided in section X.C.14, below.

- f. **Element 1[e]. “in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:”**

The Combination discloses this element. EX-1003, ¶¶167-169. Zheng discloses “in response to receiving more or more inputs, using one or more interfaces displayed on one or more computing devices” because Zheng’s system “provide[s] for interaction with a user” by implementing the system on a “computing device in communication with a display,” such as a “user interface element.” EX-1005, 13:9-18; *see also id.*, 1:48-52 (“**visualization module for rendering, on a computer display**”), 10:39-43, 13:28-37. EX-1003, ¶¶167-168.

A POSITA would understand that the “one or more computing devices” is “communicatively coupled with the one or more databases” because, as discussed

in Element 1[a], Zheng discloses “at least one **database** table is used to **store data** for **each layer** and **for each possible combination/interaction** of the layers.” EX-1005, 8:25-27; EX-1003, ¶169; Element 1[a].

- g. Element 1[f]. “using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”**

The Combination discloses this element. EX-1003, ¶¶170-173. Baker discloses importing diagrams from Microsoft Visio into a threat modeling software application. Element 1[d]. Those diagrams are stored in a Visio file (a data file) that is generated by the Visio software application. Baker explains that the Visio file comprises a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components. See EX-1006, ¶[0025]; see also *id.*, ¶¶[0009], [0023], Fig. 4.

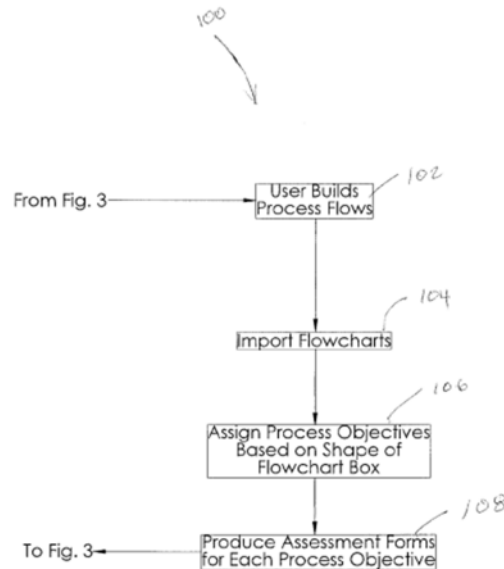


Fig. 4

A POSITA would understand that the Visio file (data file) defines one or more relationships between the subset of Visio (third party) components because the Visio components are imported as flowcharts, which are tools used to define relationships between components. EX-1003, ¶171. A POSITA would further understand that the Visio file must be “read” using a computing device when imported because a file needs to be read to be imported. *Id.*

A POSITA would further understand that Zheng discloses that the one or more interfaces is “displayed on one or more computing devices.” Element 1[e]; EX-1003, ¶¶172-173.

- h. 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;”

The Combination discloses this element. EX-1003, ¶¶174-176. 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. EX-1005, 2:38-42. Zheng further discloses that a threat target and a threat actor are associated together in a visualization display layers, where “**new** routes and/or applications” may be added to the base layer, and “and preexisting route(s) are present to connect the threat agent to the **target application**,” which may then “automatically predict new attack routes.” EX-1005, 5:35-37. In other words, Zheng’s system adds new suites of applications to the base layer and associates those applications to “target applications,” *i.e.*, correlated threat model components.

Zheng further discloses that this task is completed “using the one or more computing devices” because Zheng discloses that its system may be implemented on a computer. *See* Element 1[a].

Zheng further discloses that the correlated threat model components are “defined in the one or more mapping files” because Zheng discloses that “[a] threat can provide one-to-one **mapping between a threat actor and a threat target**.” EX-

1005, 5:20-24. The “threat targets” or threat model components are therefore defined by the mapping file.

- i. **Element 1[h]. “displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”**

The Combination discloses this element. EX-1003, ¶¶177-178. Zheng discloses “displaying ... a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model” because Zheng discloses that “[a] threat can provide one-to-one *mapping between a threat actor and a threat target.*” EX-1005, 5:20-24. Zheng’s mapping involves “*visualizing in a computer display*, as components in a base layer on a map, the suite of software applications and relationships among the software applications, automatically identifying one or more security threats in the suite of software applications, and *graphically depicting on the computer display the one or more security threats on the map in a threat modeling layer.*” *Id.*, 2:3-10; see also *id.*, 2:36-42, Fig. 8.

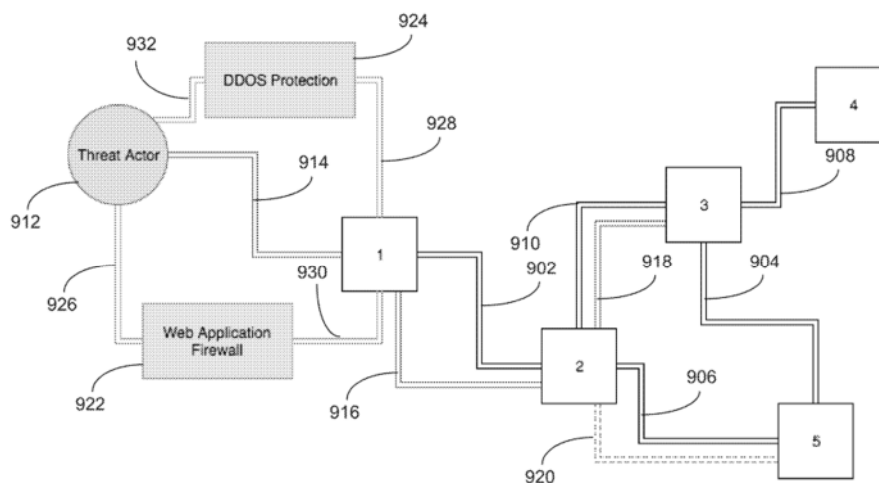


FIG. 8

Zheng further discloses that the displaying step is completed “on the one or more user interfaces” because of Zheng’s disclosures of “visualizing on a computer display” described above, and because Zheng discloses an “interactive visual interface.” *See* Element 1[e].

- j. Element 1[i]. “generating, using the one or more computing devices, and displaying, on the one or more user interfaces, 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.”**

The Combination discloses this element. EX-1003, ¶¶179-183. For example, Figure 1 of Jones discloses Reporter 114:

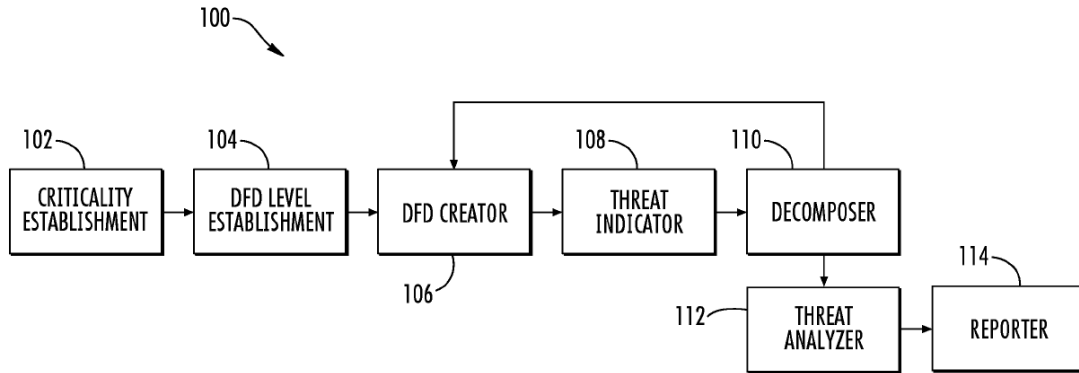


FIG. 1

Jones explains, “The reporter **114** may be configured to generate one or more reports from the threat analysis, at least one of which may include an organized arrangement of at least some of the attributes of at least some of the components, data flows or cybersecurity threat.” EX-1007, 6:59-63, Fig. 5 (report generator 502).

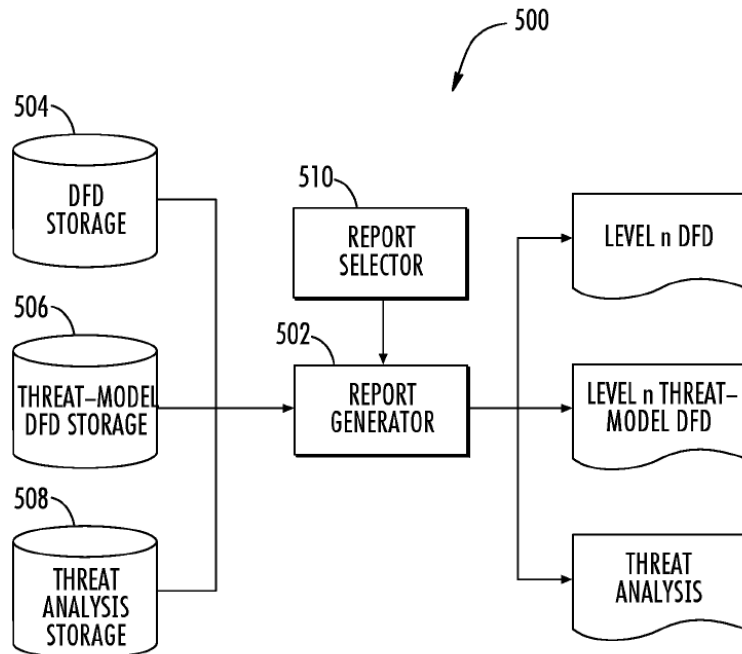


FIG. 5

Jones explains, “FIG. 5 illustrates a reporter **500**, which in some example implementations of the present disclosure may correspond to the reporter **114** of FIG. 1. ... *[T]he reporter may be configured to generate a report from the threat analysis*, and including *an organized arrangement* of at least some of the attributes of at least some of the components, data flows or cybersecurity *threat....*” EX-1007, 16:33-17:67; *see also id.*, 2:54-63, 4:25-35, 6:59-63, 18:35-37, 19:29-45, Figs. 10A-10B.

1004

1000

Numbering for this table – this does not correspond to numbering in the Visio diagram.	The weakness in the system or application that may be exploited. Can be at design, implementation, or operational level.	Event with potential adverse impact to the organization. Note that threats only need to be documented if it is deemed that there is a Current Risk.	Impact is independent of current controls or suggested mitigations.	Current security controls that mitigate the threat.	Probability that threat source will exploit the vulnerability given the current controls.	Risk given impact and current controls in place. This is an automatically calculated function of the impact and likelihood.
REF #	VULNERABILITY	THREAT	IMPACT	CURRENT CONTROLS	LIKELIHOOD	CURRENT RISK
1	Client-server connections unencrypted	Attacker may capture usernames and passwords.	Critical		Very High	Critical
2	RPC network connections not integrity-protected.	Attacker may change data using a man-in-the-middle attack.	Critical	Transmission occurs on a protected network segment available only to sys admins.	Medium	High
3	Buffer overflow finding in AppScan	Attacker may impersonate a system administrator.	Critical		Medium	High
4	Password authentication	System administrator may be impersonated.	High	Complex password policy	Medium	Medium
5	No failover system.	Failure of primary system will result in unavailability of functionality.	Medium		Medium	Medium
6	No vetting process for administrators	Improper access to system	High	Manager Approval	Low	Low
7	Admin actions not logged.	Rogue admin may subvert system with no forensic detection possible.	Low		Low	Low
8	Host-based firewall off	Increased attack surface of system.	Medium	Network-based firewall protects system.	Low	Low

FIG. 10A

● YELLOW ● PURPLE ● RED ● GREEN

1004

1000

Numbering for this table - this does not correspond to numbering in the Visio diagram.	Security controls that are recommended to bring the Current Risk rating lower.	Risk given that suggested mitigations are implemented.	The data flow diagram (DFD) element(s) that the threat applies to.	Additional clarifying information. If a finding is preliminary, meaning it needs further research indicate "Preliminary" here.	Use to note whether the review process has resulted in acceptance of this threat and associated impact and risk ratings.
REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity-protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is "Undetermined" as the vulnerability is very general.	Not Reviewed

1002

●YELLOW ●GREEN

FIG. 10B

2. Claim 2: “The method of claim 1, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.”

The Combination discloses this element because Zheng discloses that its system may be implemented by a computer with any combination of front-end, back-end, and middleware components, which a POSITA would understand includes storage on a computing device. See Element 1[e]; EX-1003, ¶184; EX-1005, 13:28-37 (“The above described techniques can be implemented in a distributed computing system that includes any combination of such back-end, middleware, or front-end components.”).

3. Claim 3: The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.

The Combination discloses this element. EX-1003, ¶185. Zheng teaches that “Information used by the security risk analysis system 100 for visualizing and predicting security risks can be stored *in one or more database tables.*” EX-1005, 8:14-18; *see also* Element 1[a].

4. Claim 4: “The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file.”

The Combination discloses this element. A POSITA would understand that a Visio file is a “VSD file” or a “VSDX file” and that Baker therefore discloses the importing a VSD or VSDX file. EX-1003, ¶186; Element 1[d].

5. Claim 7: “The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files.”

The Combination discloses this element. *See* Elements 1[f]-1[g]; EX-1003, ¶187. Zheng further discloses, referring to Fig. 8, that “the numbered boxes represent applications within the ecosystem and the connections 902, 904, 906, 908, 910 *represent relationships/data flows among the applications.* The threat actor component 912 and the connections 914, 916, 918 and 920 can be a part of the threat modeling layer 204 of the multi-layered structure 200, where the

connections 914, 916, 918 and 920 illustrate the impact of the threat actor 912 on various components of the base layer 202.” EX-1005, 11:59-68;12:1-3.

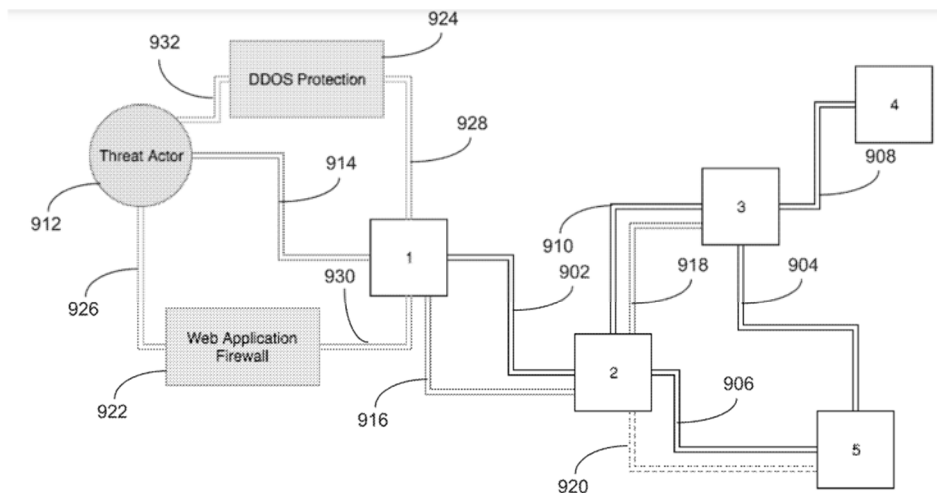


FIG. 8

6. Claim 8:

a. Element 8[p] (see Ground 1 for text of this element).

The Combination discloses this element. A POSITA would understand that Zheng’s one or more databases is communicatively coupled with one or more computing devices because Zheng discloses that its methods and systems are implemented by a computer and that “at least one **database** table is used to **store data** for **each layer** and **for each possible combination/interaction** of the layers.” *Id.*, 21:26-33; Elements 1[p]-1[a] and 1[e]; EX-1003, ¶188.

b. Element 8[a] (see Ground 1 for text of this element).

The Combination discloses this element. See Elements 1[b].

c. **Element 8[b] (see Ground 1 for text of this element).**

The Combination discloses this element. See Elements 1[c]-1[d].

d. **Element 8[c]. “an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by one of the one or more computing devices, the data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”**

The Combination discloses this element. EX-1003, ¶¶191-192; see Elements 1[e]-1[f]. Baker discloses an import interface displayed on the screen of the computing device to initiate the reading of the Visio file in response to a user input. Baker teaches that “risk management or control flowcharts *may be imported at step 104 from third party software such as that marketed as Microsoft Office Visio®*. ... At step 106, the processor 20 acts to automatically assign or associate predetermined objectives or controls according to the shapes of the imported flowcharts.” EX-1006, ¶[0025], see also *id.*, ¶¶[0009], [0023], Fig. 4.

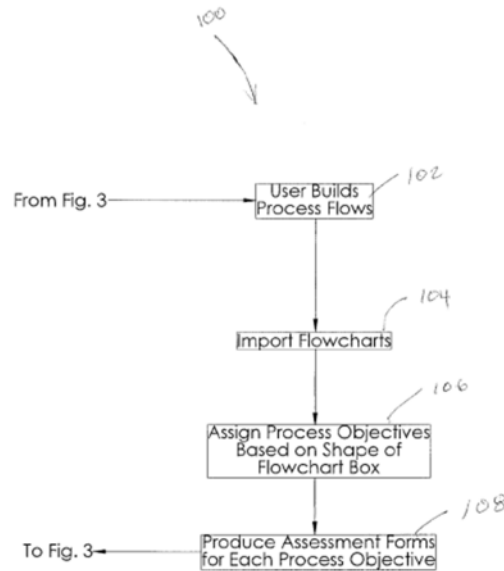


Fig. 4

EX-1003, ¶191.

A POSITA would understand import function to be an import interface displayed on a computing device as claimed because it allows a user to import third party diagram components, *e.g.*, Visio flowcharts, which are included in a data file. EX-1003, ¶192. A POSITA would further understand that Baker’s import interface initiates reading of the data file when imported. EX-1003, ¶192.

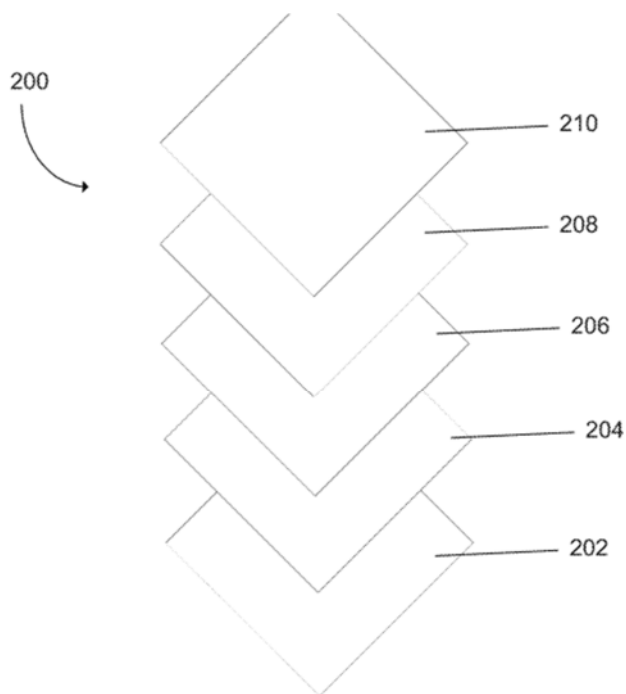
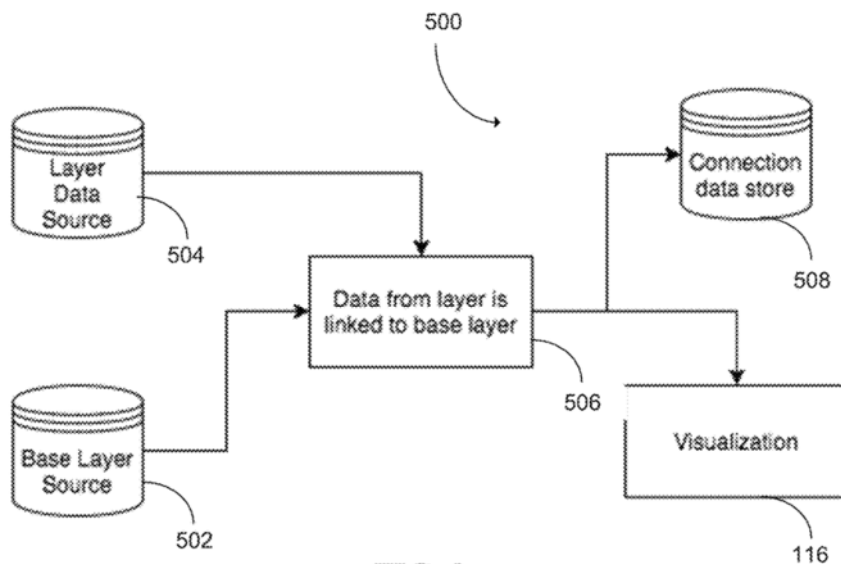
e. Element 8[d] (see Ground 1 for text of this element).

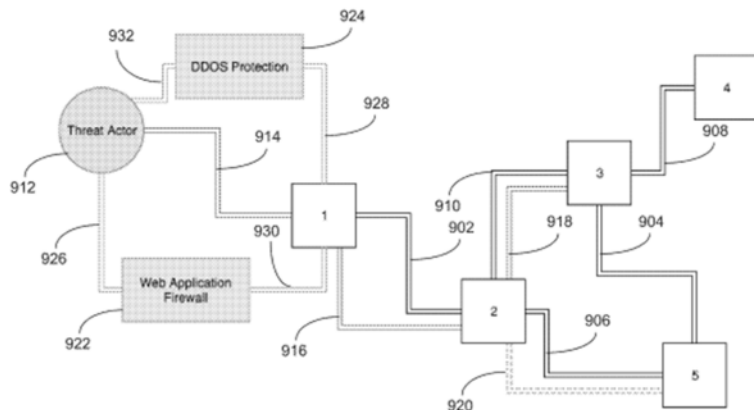
The Combination discloses this element. EX-1003, ¶¶193-194; *see* Elements 1[g], 1[d], 1[e]. Zheng discloses “an interface” because Zheng discloses an **“interactive visual interface.”** EX-1005, 10:39-43; Element 1[e].

Zheng further teaches that the interface is “configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files” because Zheng discloses a “**map**” that defines relationships between the third party components and among other system components. EX-1005, 2:38-42. Zheng further discloses that a threat target and a threat actor are associated together in a visualization display layers, where “**new** routes and/or applications” may be added to the base layer, and “and preexisting route(s) are present to connect the threat agent to the **target application**,” which may then “automatically predict new attack routes.” EX-1005, 5:35-37. In other words, Zheng’s system adds new suites of applications to the base layer and associates those applications to “target applications,” *i.e.*, correlated threat model components. Element 1[g]; EX-1003, ¶194.

f. Element 8[e] (see Ground 1 for text of this element).

The Combination discloses this element. EX-1003, ¶¶195-196; *see* Element 1[h]. A POSITA would understand that the Zheng’s disclosures discussed in Element 1[h] also disclose “a diagram interface” because Zheng discloses “**graphically depicting on the computer display the one or more security threats on the map in a threat modeling layer**,” and allowing the user to interact with the display. EX-1005, 2:3-10, 2:36-42, Fig. 8, 8:14-24; Element 1[h].





A POSITA would understand that this element is “displayed on the one or more computing devices.” See Element 1[e]; EX-1003, ¶196.

g. **Element 8[f]** (see Ground 1 for text of this element).

The Combination discloses this element. EX-1003, ¶197; see Element 1[i].

A POSITA would understand that the Jones' disclosures discussed in Element 1[i] also disclose "a threat report interface" because Jones discloses that "FIG.

5 illustrates a reporter **500**, which in some example implementations of the present disclosure may correspond to the reporter **114** of FIG. 1. ... *[T]he reporter may be*

configured to generate a report from the threat analysis, and including an

organized arrangement of at least some of the attributes of at least some of the components, data flows or cybersecurity threat....” EX-1007, 16:33-17:41. A

POSITA would understand that Jones' reporter configured to generate a report by a user is a threat report interface as claimed.

7. Claim 9 (see Ground 1 for text of this element).

The Combination discloses this element. *See* Claim 2.

8. Claim 10 (see Ground 1 for text of this element).

The Combination discloses this element. *See* Claim 3.

9. Claim 11 (see Ground 1 for text of this element).

The Combination discloses this element. *See* Claim 4.

10. Claim 15: The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files.

The Combination discloses this element. EX-1003, ¶200. Zheng discloses “one or more mapping interfaces displayed on the one or more computing devices.” *See* Element 1[e], 1[h]. Zheng further discloses “one or more mapping interfaces ... configured to, in response to receiving user input, modify the one or more mapping files” because Zheng discloses that a “user can interact with the resulting visualization” of the user interface to modify the display, *i.e.*, “to achieve the desired display effects.” EX-1005, 11:41-49 (“the threat modeling layer ... has sub-categories in the layer that can be **toggled** (e.g., enabled or disabled) by the user.”); *see also id.* 11:49-55 (“the visualization module 116 allows panning and/or zooming of the visualized structure.”). A POSITA would understand that modifications to the display likewise modify the mapping file. EX-1003, ¶200.

11. Claim 16:

a. Element 16[p]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Elements 1[p]-1[a], 1[e], and 8[p].

b. Element 16[a]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Elements 1[a] and 8[a].

c. Element 16[b]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Elements 1[c]-1[d] and 8[b].

d. Element 16[c]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Element 8[c].

e. Element 16[d]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Element 1[g] and 8[d].

f. Element 16[e]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Element 1[h] and 8[e].

g. Element 16[f]. (see Ground 1 for text of this element).

The Combination discloses this element. *See* Element 1[i] and 8[f].

12. Claim 17 (see Ground 1 for text of this element).

The Combination discloses this element. *See* Claim 2.

13. Claim 18 (see Ground 1 for text of this element).

The Combination discloses this element. *See* Claim 3.

14. A POSITA Would Have Been Motivated to Combine Zheng With Baker and Jones.

A POSITA would have been motivated to combine Zheng, Baker, and Jones. First, like the '366 patent, all three references relate to the same general subject matter of generating threat models on a computer. *See* EX-1005, Abstract; EX-1006, Abstract, EX-1007, Abstract; EX-1003, ¶210.

Second, Zheng provides express motivation when it discusses the need to minimize the tedious burden on human beings that exists in certain prior art threat modeling software applications:

With the growing complexity of application architecture and application infrastructure, it becomes tedious and often unmanageable to analyze application security across a large portion or an architectural stack. Today's threat modeling applications are often static and require either manual input or antiquated approaches to account for new architecture, code and/or infrastructure....

Accordingly, there is a need for improved systems, methods and apparatuses for a more effective and efficient threat modeling approach in the context of application architecture and infrastructure.

EX-1003, 1:21-34. Adding the teachings of Baker and Jones to the system disclosed in Zheng would further Zheng's stated goal of an improved threat modeling system. For example, Zheng recognizes the need to produce threat models faster (in real time or near real time) and using easy-to-understand visualizations. EX-1:37-45; EX-1003, ¶212. Thus, a POSITA would be motivated to combine these references because the ability to import existing

diagrams from Visio, as taught in Baker, and the ability to generate threat reports, as taught in Baker and Jones, would reduce amount of tedious and unmanageable work that human operators would otherwise need to handle and provide commonplace, easy-to-understand visualizations. EX-1003, ¶¶211-212; EX-1005, 1:37-45; EX-1011

Third, Microsoft Office Visio was a well-known software tool for generating flowcharts and diagrams at the time the patents were filed. *E.g.*, EX-1007, 18:30-43. A POSITA would have been motivated to allow users to take existing diagrams already prepared in Visio and import those diagrams into the system of Zheng. EX-1003, ¶213. Users were already comfortable with Visio, which has many good features and is easy to use. This would allow users to create threat models from diagrams already created in Visio to save time of creating those same diagrams using a native interface in the Zheng system. *Id.*

In general, compatibility between software programs is a positive improvement that users appreciate. *E.g.*, EX-1007, 18:30-43 (noting compatibility between Jones' system and Microsoft Visio). For example, it is commonplace today to use one program, such as Adobe Acrobat, to create a pdf and to import that pdf into a second program such as a Microsoft PowerPoint presentation. *Id.* (discussing Jones' system is also compatible with Excel and other commonplace programs). Similarly, users would benefit from being able to import a Visio

diagram into the threat modeling tool of Zheng. EX-1003, ¶214. For example, a POSITA would readily understand that Zheng's mapping file would be useful in mapping the relationships between the imported Visio diagrams.

Fourth, the threat model reports of Jones are a useful feature. Reports are efficient mechanisms for humans to digest complicated sets of data. A POSITA would have been motivated to combine Zheng with the report generation feature of Jones so that a user of the Zheng system could have reports to quickly understand threat models and potential threats to underlying systems. EX-1003, ¶215.

Combining these references would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Further, such a combination would have an easily predictable result. Accordingly, a POSITA would have had a reasonable expectation of success. EX-1003, ¶216.

D. Ground 3: The References of Ground 2 in Further View of Galliano Render Obvious Claims 2, 9, and 17

Claims 2, 9, and 17 are rendered obvious by the references of Ground 2 in further view of Galliano. EX-1003, ¶¶217-220. Galliano discloses the elements of claims 2, 9, and 17 in Figure 3, which states that the “[m]odel is *either stored in a back-end repository (ex. database) or in memory within a computing system*”:

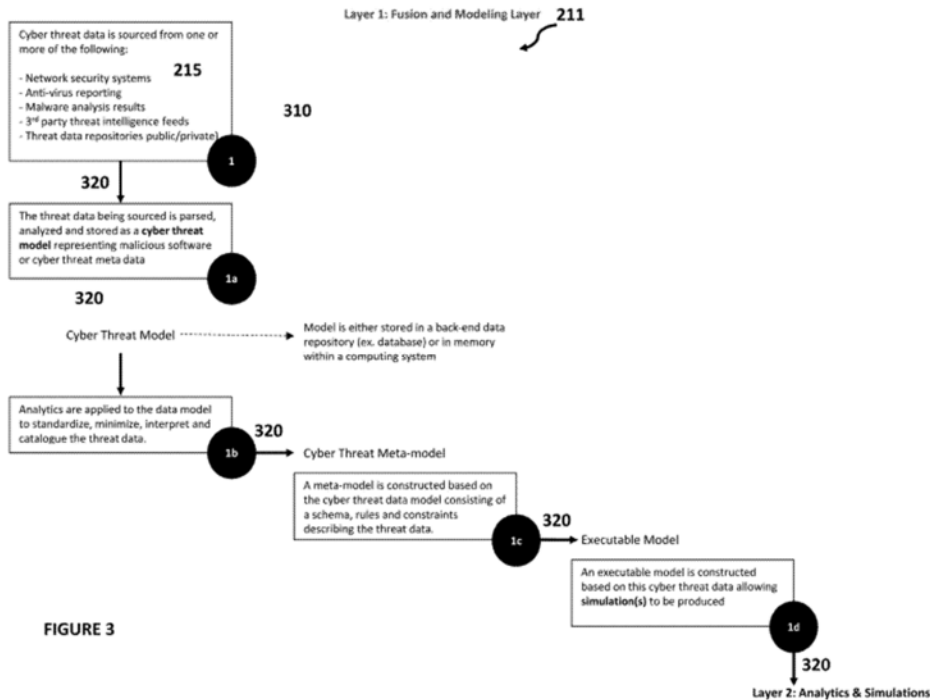


FIGURE 3

EX-1008, Figure 3.

A POSITA would have been motivated to combine Zheng, Baker, Jones, and Galliano for the same reasons discussed in Ground 2 for Zheng, Baker, and Jones. Galliano also relates to the general subject matter of generating threat models on a computer. See Ground 2; EX-1008 at Abstract; EX-1003, ¶218.

Furthermore, a POSITA would have been specifically motivated to combine the teachings of Galliano with the system of Zheng. Galliano teaches that mapping files can be stored either in a database or in a computing device without using a database. EX-1008, Figure 3. A POSITA would understand that mapping files in the Zheng system need to be stored and would have used Galliano's teaching that

the mapping files can be stored in a database or elsewhere in a computer system.

EX-1003, ¶219.

Combining these references would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Further, such a combination would have an easily predictable result. Accordingly, a POSITA would have had a reasonable expectation of success. EX-1003, ¶220.

E. Ground 4: The References of Ground 2 in Further View of Keenan Render Obvious Claims 1-20

Claims 5-6, 12-14, and 19-20 describe the use of certain names and titles for third-party components in the threat model. These claims are rendered obvious by the references of Ground 2 in further view of Keenan. EX-1003, ¶¶221-223. As shown in Ground 1, Keenan expressly discloses the elements of those claims as well as claims 1-4, 7-11, and 15-18.

A POSITA would have been motivated to combine the teachings of Keenan with the system of Zheng, Baker, and Jones for the reasons discussed above for Ground 2. In addition, Keenan describes a certain naming convention for names and titles for third-party components. These are mere design choices that would have been obvious to a POSITA, and they are expressly disclosed in Keenan. A POSITA would understand that names and titles were required, and Keenan discloses this specific aspect. EX-1003, ¶222.

Combining these references would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Further, such a combination would have an easily predictable result. Accordingly, a POSITA would have had a reasonable expectation of success. EX-1003, ¶223.

F. Ground 5: The References of Ground 2 in Further View of the Knowledge of a POSITA Render Obvious Claims 2, 5-6, 9, 12-14, 17, and 19-20

Claims 2, 5-6, 9, 12-14, 17, and 19-20 are rendered obvious by the references of Ground 2 in further view of the knowledge of a POSITA. EX-1003, ¶¶224-227.

A POSITA would have understood that mapping files can be stored in a database or in a computing device without using a database as specified in claims 2, 9, and 17. This would have been immediately clear to a POSITA at the relevant time, and a POSITA would understand that mapping files need to be stored and that as a matter of mere design choice, they could be stored in a database or in a mechanism that does not require a database, such as a file system. A POSITA might choose to use a database in some situations and a file system in others. For example, databases are efficient tools when there the volume of data is significant and if search capabilities are desired. However, databases also require database software, which would add to the overall cost of the underlying a system. A POSITA therefore might choose to store the mapping files in a file system and not

in a database to save on the costs of the overall system or if there are not many mapping files being used or if search capability is not important. EX-1003, ¶225.

A POSITA would have understood that third-party components can be named or titled in a certain way as specified in claims 5, 6, 12-14, and 19-20 as a matter of mere design choice. EX-1003, ¶226.

Modifying Zheng, Baker, and Jones in this manner with the knowledge of a POSITA would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Further, such a combination would have an easily predictable result. Accordingly, a POSITA would have had a reasonable expectation of success. EX-1003, ¶227.

XI. THIS PETITION IS PROPER UNDER 35 U.S.C. §§ 314(a) AND 325(d)

The *Fintiv* factors weigh against discretionary denial. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

A. Stay

Petitioner intends to promptly seek a stay of the Litigation if the Board institutes this proceeding. This factor weights against discretionary denial, or at worst, is neutral.

B. Trial Date

The deadline for a Final Written Decision will be around September 2024. In the Litigation, the Court has not yet set a *Markman* hearing or a trial date. A June 30, 2022 report from Federal Judiciary indicates that the median time from

filing to trial in the District of Delaware where the Litigation is pending is 36.0 months, EX-1009, which would place trial in the Litigation at July 8, 2025, nearly ten months after the Final Written Decision would be issued in this IPR. This factor weighs against a discretionary denial.

C. Parallel Proceeding

In *Sand Revolution*, the parties had already exchanged infringement and invalidity contentions, and the court had issued a *Markman* Order. *Sand Revolution II, LLC v. Continental Intermodal Grp. - Trucking LLC*, IPR2019-01393, Paper 24 (June 16, 2020) (informative). Despite these facts, the Board found that the third *Fintiv* factor “weighs only marginally, if at all, in favor of exercising discretion to deny institution.” *Id.* Here, the Litigation is at a drastically earlier phase. This factor weighs against discretionary denial.

D. Issue Overlap

Petitioner has stipulated that, to the extent the Board institutes this IPR Petition, Petitioner will not pursue in the Litigation the grounds raised in this Petition. EX-1010. Moreover, the prior art in the Litigation will include a substantial number of references not at issue in this IPR. This factor weighs against discretionary denial.

E. Same Party

Petitioner and the PO are the parties in the Litigation. However, members of the Board have noted that *Fintiv* “says nothing about situations in which the

petitioner is the same as, or is related to, the district court defendant.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15, at *10 (PTAB May 15, 2020) (APJ Crumbley, dissenting). This factor is neutral.

F. Other Considerations

The ’366 patent has never been challenged in a post-issuance proceeding, and the references used herein were not cited during prosecution. This factor weighs against discretionary denial.

Moreover, this Petition presents compelling unpatentability challenges that warrant institution. *See* USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation.

XII. CONCLUSION

Petitioner has shown a reasonable likelihood of prevailing on claims 1-20 and requests institution of *inter partes* review and cancellation of these claims.

Respectfully submitted,

Dated: March 7, 2023

/Brent Yamashita/
Brent Yamashita

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(c) and (d), Petitioner certifies that the word count of Petitioner's Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, mandatory notices under § 42.8, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 13,947 words.

By: /Brent Yamashita/
Brent Yamashita

CERTIFICATE OF SERVICE ON PATENT OWNER

UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that, on March 7, 2023, a complete and entire copy of this Petition for *Inter Partes* Review, together with all supporting exhibits, were served on Patent Owner electronically, by agreement, by emailing a copy of the same to the following attorneys for the Patent Owner:

whelge@davidsonberquist.com
jwilson@davidsonberquist.com
esong@davidsonberquist.com

By: /Brent Yamashita/
Brent Yamashita