IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

THREATMODELER SOFTWARE INC., Plaintiff, v. IRIUSRISK, INC., and IRIUSRISK, S.L., Defendants.	C.A. No. _____ **JURY TRIAL DEMANDED**

PLAINTIFF THREATMODELER SOFTWARE INC.'S COMPLAINT
FOR PATENT INFRINGEMENT

Plaintiff ThreatModeler Software Inc. ("ThreatModeler"), by and through its attorneys, hereby alleges this Complaint against Defendant IriusRisk, Inc. and Defendant IriusRisk, S.L. (collectively, "IriusRisk" or "Defendants") for patent infringement.

PARTIES

1. Plaintiff ThreatModeler is a corporation organized and existing under the laws of the State of Delaware and having a principal place of business at 101 Hudson St., Suite 2100, Jersey City, New Jersey 07302.

2. Upon information and belief, Defendant IriusRisk, Inc., is a Delaware corporation and has its principal place of business at 1290 Orange Street, Wilmington, Delaware 19801. IriusRisk can be served in the State of Delaware through its registered agent, the National Registered Agents, Inc., located at 1209 Orange Street, Wilmington, Delaware, 19801.

3. Upon information and belief, Defendant IriusRisk, S.L. is a Spanish company having its principal place of business in Spain.

4. ThreatModeler is the sole and exclusive owner of U.S. Patent No. 11,314,872, titled "Systems and Methods for Automated Threat Modeling when Deploying Infrastructure as a

Code" ("the '872 Patent" or the "Asserted Patent"). A true and correct copy of the '872 Patent is attached as Exhibit A.

5. On April 26, 2022, the United States Patent and Trademark Office duly and legally issued the '872 Patent. ThreatModeler is the owner by assignment of all right, title and interest in and to the '872 Patent, including the right to sue, enforce and recover damages for all past, present, and future infringements of the patent.

6. IriusRisk makes uses, sells, offers for sale, and/or imports in the United States, including in this judicial district, products and/or services that directly and indirectly infringe at least claims 1-6, 11-14, 16-21, and 26-29 of the '872 Patent, either literally or under the doctrine of equivalents. These products and/or services include but are not limited to IriusRisk's Threat Modeling Platform (both the cloud-based version and the on-premises version) including its Infrastructure as a Code ("IaC") functionality and/or StartLeft functionality made, used, offered for sale, sold, and/or imported on or after April 26, 2022 (collectively, the "Accused Instrumentalities").

JURISDICTION AND VENUE

7. This is an action for patent infringement, arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.*

8. This Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

9. Defendant IriusRisk, Inc. is a company organized under the laws of the State of Delaware and is subject to this Court's specific and general personal jurisdiction. IriusRisk, Inc.'s registered agent in Delaware is National Registered Agents, Inc., 1209 Orange Street, Wilmington, Delaware 19801.

10. Defendant IriusRisk, S.L. is a company organized under the laws of Spain and is subject to this Court's specific and general personal jurisdiction.

11. Defendants IriusRisk, Inc. and IriusRisk, S.L. have committed and induced acts of infringement within the state of Delaware, as alleged herein, and have derived substantial revenues and benefits from their infringing acts occurring within Delaware.

12. Defendants maintain continuous and systematic contacts within this district by offering for sale, selling and otherwise providing the Accused Products (and components thereof) to residents, customers, potential customers, and users within this district.

13. Defendant IriusRisk, Inc. is an agent of IriusRisk, S.L. at least insofar as IriusRisk, Inc. is a sales and/or support agent of IriusRisk, S.L. The actions, residence, and conduct of IriusRisk, Inc. are attributable to IriusRisk, S.L. at least due to IriusRisk, Inc.'s status as an agent of IriusRisk, S.L. IriusRisk, Inc. and IriusRisk, S.L. have common management and have at least one common officer or director. IriusRisk, Inc. and IriusRisk, S.L. are under common control. IriusRisk, Inc.'s activities are materially directed by IriusRisk, S.L. or its officers or directors.

14. Defendants IriusRisk, Inc. and IriusRisk, S.L. use and offer to its customers and users, within the state and District of Delaware, the Accused Products. Defendants IriusRisk, Inc. and IriusRisk, S.L. also solicit customers and potential customers within the state and District of Delaware via their internet presence, and on information and belief, offer to provide and actually provide demonstrations of its Accused Products to customers, potential customers, and users within the state and District of Delaware.

15. IriusRisk provides, owns, maintains, and operates a collection of websites and Internet storage repositories through which the Accused Products are offered for sale, sold, and

otherwise provided to customers, potential customers, and users within the state and District of Delaware ("IriusRisk Websites"). The IriusRisk Websites include, but are not limited to, those found at the following URLs: https://www.iriusrisk.com/, https://community.iriusrisk.com/, https://enterprise-support.iriusrisk.com/s/, https://www.threatmodelingconnect.com/, and https://www.threatmodcon.com/ and subdomains of these URLs. The IriusRisk Websites further include IriusRisk's YouTube channel, IriusRisk's GitHub repositories, and IriusRisk's Dockerhub repositories. IriusRisk intends to serve the United States market with its Accused Products including the Delaware market. IriusRisk's intent to serve the United States market results in the Accused Products being offered for sale, sold, and otherwise provided to customers, potential customers, and users within the state and District of Delaware. IriusRisk offers for sale, sells, and otherwise provides the Accused Products to residents, customers, potential customers, and users within the state and District of Delaware through its established Internet channels and websites knowing and intending for the Accused Products to be offered for sale, sold, and otherwise provided to residents, companies, and individuals in Delaware so that those residents, companies, and individuals can consider purchasing the Accused Products and use the Accused Products. IriusRisk purposefully directs information regarding the Accused Products via one or more of the IriusRisk Websites to the United States market including Delaware for the education of residents, customers, potential customers, and users within the state and District of Delaware. IriusRisk also purposefully directs files relating to the Accused Products via one or more of the IriusRisk Websites to the United States market including Delaware for the download, installation and/or use of the Accused Products or components thereof by residents, customers, potential customers, and users within the state and District of Delaware. IriusRisk also purposefully directs files, such as application files, information

tracking files, and interactive cookie files, to residents, customers, potential customers, and users within the state and District of Delaware from one or more of the IriusRisk Websites to provide the Accused Products (or components thereof), obtain information about website visitors, to keep a record of website visitor browsing habits, website visitor preferences, and website visitor login information and identity for the purpose of facilitating its business including providing the Accused Products (or components thereof), information about the Accused Products, and the use of the Accused Products.

16. IriusRisk conducts business in the state and District of Delaware including the sale, offer for sale, and use of the Accused Products through the IriusRisk Websites. Upon information and belief, residents of Delaware have logged into one or more of the IriusRisk Websites to obtain information about the Accused Products and/or to download or use the Accused Products.

17. Upon information and belief, IriusRisk has offered for sale and sold the Accused Products to residents of Delaware including Delaware corporations. Examples of Delaware residents to which IriusRisk has sold and offered for sale the Accused Products include DocuSign, Inc. (a Delaware corporation), United Parcel Service, Inc. (a Delaware corporation), and Verizon Communications Inc. (a Delaware corporation). Each sale and each offer for sale to Delaware residents are individual acts of patent infringement occurring in this district. Each such sale and each such offer for sale have caused and continue to cause harm to ThreatModeler in this district at least because ThreatModeler is a Delaware corporation.

18. IriusRisk's Websites provide a portal through which potential customers, including residents of Delaware, can request pricing information for the Accused Products. Upon information and belief, IriusRisk also provides email addresses which are through

subdomains of one or more of the IriusRisk Websites through which customers and potential customers, including residents of Delaware, can request and obtain pricing information for the Accused Products. Upon information and belief, IriusRisk provides pricing information via electronic mail subdomains to one or more of the IriusRisk Websites.

19. Upon information and belief, IriusRisk provides customers and potential customers, including residents of Delaware, with login information and credentials which allow those customers and potential customers to download and/or use the Accused Products (or components thereof) via one or more of the IriusRisk Websites or subdomains thereof.

20. Residents, customers, potential customers, and users within the state and District of Delaware who access or use the IriusRisk Websites are subject to IriusRisk's Legal Notice & Website Terms of Service, IriusRisk's Privacy Policy, and IriusRisk's Cookie Policy for the IriusRisk Websites that each create contractual rights and obligations for IriusRisk and each resident, customer, potential customer, and user of the IriusRisk Websites, including residents, customers, potential customers, and users in Delaware.

21. On information and belief, IriusRisk, S.L. owns, controls, and directs IriusRisk, Inc. IriusRisk, S.L. uses IriusRisk, Inc. to perform one or more of the infringing activities described herein and derives substantial revenue therefrom. IriusRisk, S.L. and IriusRisk, Inc. share one or more common officers and/or directors.

22. For these reasons, personal jurisdiction exists and venue is proper in this District and Court under 28 U.S.C. § 1400(b), and for IriusRisk, S.L., venue is proper under 28 U.S.C. § 1391(c)(3).

THREATMODELER'S INNOVATIONS AND PATENTS

23. ThreatModeler is a cybersecurity company that has developed automated threat

modeling solutions for fortifying an enterprise's software development lifecycle. ThreatModeler's solutions identify, predict and define threats in order to educate security and development teams to incorporate countermeasures during any phase of the software development lifecycle, including early in software and system development.

24. The cybersecurity applications for ThreatModeler's threat model solutions include but are not limited to medical fields, finance, and retail.

25. ThreatModeler's threat model solutions allow for the generation of threat model using or based on IaC files and/or functionality. ThreatModeler's solutions allow more robust threat modeling, more comprehensive identification and analyses of threats, and identification of weaknesses and countermeasures based on identified threats.

26. ThreatModeler has collected numerous awards for its ThreatModeler platform, including being named "Most Innovative" by Cyber Defense Magazine's InfoSec Awards in 2018. ThreatModeler was awarded Cyber Defense Magazine's InfoSec Award in 2018, 2019, and 2021. ThreatModeler was awarded CyberSecurity Excellence Awards in 2017, 2018, 2019, and 2020. ThreatModeler was awarded the Big Innovation Award in 2021, and was a Digital Revolution Awards winner in 2021.

27. On May 16, 2022, ThreatModeler was named an SC Magazine Awards Finalist for Best Threat Intelligence Technology. SC Magazine reported that "Cybercrime is big business, and techniques of bad actors are growing increasingly sophisticated. That leaves security teams thirsting for near realtime intelligence about the threat landscape." *See* https://www.scmagazine.com/news/threat-intelligence/finalists-best-threat-intelligence-technology. In recognizing ThreatModeler's technical achievements, SC Magazine reported: "ThreatModeler is a collaborative platform where security experts or non-security professionals

alike can build threat models within a few hours or minutes instead of weeks through a completely automated process. The latest evolution of ThreatModeler's technology delivers real-time threat modeling capabilities, enabling developers to understand the full scope of their intended IT infrastructure." *Id*.

28. ThreatModeler has been granted multiple U.S. patents for various inventions including threat modeling functionality, systems, and methods.

29. In 2017, ThreatModeler filed four provisional patent applications directed to threat modeling methods and systems. ThreatModeler filed U.S. Provisional Application No. 62/530,295 on July 10, 2017. ThreatModeler filed U.S. Provisional Application No. 62/527,671 on June 30, 2017. ThreatModeler filed U.S. Provisional Application No. 62/520,954 on June 16, 2017. And ThreatModeler filed U.S. Provisional Application No. 62/507,691 on May 17, 2017. Collectively, these four U.S. provisional applications are referred to hereinafter as the "Provisional Applications."

30. ThreatModeler's '872 Patent was filed on September 20, 2021 as U.S. Patent Application No. 17/479,815, which is a continuation-in-part application of U.S. Patent Application No. 16/950,509, filed on November 17, 2020 (which issued as U.S. Patent No. 11,159,559), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 16/947,798, filed on August 17, 2020 (which issued as U.S. Patent No. 10,984,112), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 16/664,679, filed on October 25, 2019 (which issued as U.S. Patent No. 10,747,876), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 16/228,738, filed on December 20, 2018 (which issued as U.S. Patent No. 10,699,008), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 15/922,856, filed on March

15, 2018 (which issued as U.S. Patent No. 10,200,399), which in turn is a continuation-in-part application of U.S. Patent Application Ser. No. 15/888,021, filed on February 3, 2018 (which issued as U.S. Patent No. 10,255,439). The '872 Patent also claims priority from and the benefit of the Provisional Applications. *See* Ex. A.

OVERVIEW OF U.S. PATENT NO. 11,314,872 AND BENEFITS OF THE INVENTIONS

31. The '872 Patent is titled: "Systems and Methods for Automated Threat Modeling when Deploying Infrastructure as a Code." The '872 Patent discloses and claims innovative solutions for developing threat models via IaC files, descriptors, and functionality.

32. The '872 Patent discloses exemplary benefits and advantages for creating threat models using IaC: "The systems & methods described herein may also be used for deploying cloud computing architectures using infrastructure as code (IAC) processes. When deploying the architecture, development and dev-ops team members may utilize infrastructure as a code technique to identify, articulate and deploy resources within the cloud computing environment. Conventionally, security threats and concerns are ignored in IAC processes. Therefore, in implementations discussed above the deployed system is analyzed for threats upon completion of the resource deployment." *See* '872 Patent, col. 39:38-47.

33. The '872 Patent discloses other exemplary benefits and advantages for creating threat models using IaC including: "When deploying a resource one or more of the following factors may be taken into consideration: the resource or service; the resource or service type; details of the resource 50 or service such as name, tags, required properties, templatized resource or service structures, reference resources or services; and resource or service properties including security properties and non-security properties. Some resource or service properties are directly attributable to the resource or service itself. For example, turning on accidental termination

protection for EC2 while deploying a resource "EC2 Instance" would be considered a directly attributable property. Other resource or service properties need to be indirectly mapped to the resource. The indirect mapping can be performed in various ways: through subproperties; through other resource properties; through other service properties; or through communication links. Indirect mapping using sub-properties may be performed where individual properties further contain a varying combination of sub-parameters that need to be defined. For example: when coding a new ELB, for default rule, the property Listener has two sub-properties- AuthenticateCognitoConfig OR AuthenticateOidcConfig. Thus, during coding, AWS: :ElasticLoadBalancingV2: :Listener>>Default actions>>AuthenticateCognitoConfig OR AuthenticateOidcConfig should be set." *See* '872 Patent, col. 39:48-40:5.

34. The '872 Patent discloses other exemplary benefits and advantages for creating threat models using IaC including: "Indirect mapping using other resource properties may be performed where an individual property is dependent on other resources being configured to either communicate or work in line with the source resource. For example, when spinning up a resource called EC2 Instance, the Security Group resource needs to be associated with the EC2 Instance resource and configured appropriately. Indirect mapping using other service properties may be performed where an individual property is dependent on properties of other services. For example, to encrypt data at rest for a database resource, a user needs to identify encryption certificates which are stored within a certificate management system (and this system is a separate service). Indirect mapping using communication links may be performed where an individual property is dependent on communication links being derived between two services or resources. For example, for an EC2 instance to communicate internally with any other service, HTTP or HTTPS communication links have to be identified and associated with the EC2

instance." *See* '872 Patent, col. 40:6-25.

35. The '872 Patent discloses other exemplary benefits and advantages for creating threat models using IaC including: "Often, a user responsible for deploying architectures would also use templates of codes that are readily available within the organization, rather than writing the code themselves. However, in either case, the aspect of securely deploying the architectures is missed. The user is not aware of security threats or attack pathways that may be introduced into the architecture as resources are being deployed. In implementations an assisted IAC design system may include interfaces that permit a user to understand, at the time of writing code for deploying infrastructure, the various security parameters that may need to be addressed. A user responsible for deploying architectures could also perform updates to an existing architecture by submitting an updated IAC. The user in this case will utilize reference points in the existing architecture and further provide properties or sub-properties that need to change. In implementations, the system may use the rules stored in a knowledge database to identify security vulnerabilities associated with the resource being updated and also identify the resource/ service being referred to in the updated IAC. In implementations, the system will identify the referred resource/service, the details of which are stored in a database which contains configuration information of all deployed architectures. *See* '872 Patent, col. 40:26-49.

THE CLAIMS OF THE '872 PATENT ARE ELIGIBLE FOR PATENTING

36. The claims of the '872 Patent are directed to improvements in how threat modeling may be performed on a computer, including by using IaC to generate threat models, and do not merely invoke the basic idea to use a computer to implement a threat model.

37. The benefits and improvements of the systems and methods claimed in the '872 Patent include those recited above in paragraphs 31-35.

38. Threat modeling in the manner disclosed and claimed in the '872 Patent was not well known, routine, and conventional. Rather, the novel systems and methods claimed include improvements over conventional threat modeling systems and methods.

39. Further, the ordered combinations claimed in the '872 Patent recite inventions that are not merely the routine or conventional use of a computer. These claims are directed to the novel threat modeling systems and methods using IaC.

IRIUSRISK'S NOTICE OF ASSERTED PATENT AND ACTIONS

40. IriusRisk has been placed on constructive notice of the Asserted Patent at least by ThreatModeler's marking of its covered products (including ThreatModeler®) in compliance with 35 U.S.C. § 287(a). *See* https://threatmodeler.com/intellectual-property, https://threatmodeler.com/patents.

41. Plaintiff ThreatModeler and IriusRisk are competitors in the limited field of providing threat modeling services and solutions, and often submit competing proposals for providing threat modeling services solutions to potential customers and users. Plaintiff ThreatModeler's threat model platform (herein referred to as the "ThreatModeler Platform") has received numerous industry accolades, including those recounted in paragraphs 26-27 of this Complaint, and those awards are widely published in industry trade magazines and websites. On information and belief, IriusRisk monitors and is aware of these same industry trade magazines and websites, and is and has been aware of ThreatModeler's industry awards and accolades. On information and belief, as a direct competitor of ThreatModeler, IriusRisk also monitors and is aware of ThreatModeler's website, including the announcements of issued patents and new ThreatModeler Platform product features announced there. *See, e.g.*, https://threatmodeler.com/threatmodeler-announces-new-patent-for-iac-assist (posted June 7,

2022), https://threatmodeler.com/threatmodeler-launches-iac-assist-and-cloudmodeler-to-reduce-threat-drift-from-code-to-cloud (posted Nov. 29, 2021). Further, following the issuance of ThreatModeler's U.S. Patents and the incorporation of its patented features into its ThreatModeler Platform, IriusRisk has added similar features to its own Accused Products. For example, ThreatModeler's '872 Patent issued on April 26, 2022. The issuance of this patent was reported on by industry journalists, including by Global Security Mag on or about June 9, 2022. *See* https://www.globalsecuritymag.com/ThreatModeler-Announces-New-Patent,20220609,126371.html. Approximately two months after the issuance of ThreatModeler's '872 Patent, and after ThreatModeler and Global Security Mag publicized the issuance of ThreatModeler's '872 patent, on or about June 17, 2022, IriusRisk added a new link to its Threat Modeling Platform dropdown menu on its company home page, labeled "Infrastructure as Code" and linked to a site labeled "Infrastructure as Code (IaC)." *See* https://www.iriusrisk.com/?hsLang=en; https://www.iriusrisk.com/iac. In its IaC site, IriusRisk described features substantially similar and/or identical to those disclosed in ThreatModeler's IaC patent. On information and belief, IriusRisk has been monitoring ThreatModeler's website and granted U.S. patents, including the Asserted Patent, and was aware of ThreatModeler's granted U.S. patents prior to the filing of ThreatModeler's Complaint. On information and belief, IriusRisk was aware of the '872 Patent prior to the filing of ThreatModeler's Complaint in this action.

42. IriusRisk has actual notice of the '872 Patent no later than the date of service of ThreatModeler's Complaint.

43. In order for a user to use and benefit from IriusRisk's Accused Instrumentalities, the user must agree to and comply with the terms and conditions of a license provided by

IriusRisk, and must operate the Accused Instrumentalities in the manner provided by IriusRisk. Each user using the Accused Instrumentalities pursuant to license from IriusRisk, and in communication with one or more IriusRisk-controlled servers, benefits from IriusRisk's providing of the Accused Instrumentalities, the manner of which usage is designed and controlled by IriusRisk and conditioned on compliance with the user's license.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 11,314,872

44. ThreatModeler incorporates herein by reference the allegations stated in paragraphs 1-43 of this Complaint.

45. IriusRisk has directly infringed, either literally or through the doctrine of equivalents, at least claims 1-6, 11-14, 16-21, and 26-29 of the '872 Patent, by making, using, offering to sell, selling and/or importing products in the United States and in this judicial district, including but not limited to the Accused Instrumentalities, thereby constituting infringement under 35 U.S.C. § 271(a). *See* Ex. B, Claim Chart for U.S. Patent No. 11,314,872 which is hereby incorporated by reference as if fully set forth herein. IriusRisk's direct infringement includes, without limitation, IriusRisk's testing of the Accused Instrumentalities, and recorded and live demonstrations of the Accused Instrumentalities to its customers, potential customers, and users. Additionally, the asserted claims of the '872 Patent are directly infringed by IriusRisk because all of the user-side steps of the asserted method claims are attributable to IriusRisk.

46. To the extent any fact finder concludes that IriusRisk's Accused Instrumentalities do not literally satisfy any element of at least claims 1-6, 11-14, 16-21, and 26-29 of the '872 Patent, those elements are met under the Doctrine of Equivalents.

47. Defendants actively, knowingly, and intentionally has induced infringement of the '872 Patent under 35 U.S.C. § 271(b) through a range of activities.

48. IriusRisk has induced infringement by IriusRisk's customers and users by controlling the design and development of, offering for sale, and selling the services of the Accused Instrumentalities with the knowledge and specific intent to encourage its customers and users to use the Accused Instrumentalities in their intended manner, which infringes the '872 Patent. IriusRisk has also induced infringement of the '872 Patent by disseminating promotional, marketing, educational, demonstrative, and tutorial materials relating to the Accused Instrumentalities with the knowledge and specific intent that its customers and users will use the Accused Instrumentalities to perform threat modeling in an infringing manner. On information and belief, IriusRisk has engaged in the above activities with knowledge of the '872 Patent and with the specific intent to encourage and cause direct infringement by its customers and users. Further, IriusRisk continues to engage in the above activities with actual knowledge of the '872 Patent and with the specific intent to encourage and cause direct infringement by its customers and users.

49. Upon information and belief, since at least the time IriusRisk received notice of the '872 patent, IriusRisk has contributed to, and continues to contribute to, the infringement by third parties, including its customers, of one or more claims of the '872 patent, including at least claims 1-6, 11-14, 16-21, and 26-29, under 35 U.S.C. § 271(c), by, for example, selling and/or offering for sale the Accused Instrumentalities in the United States and in this judicial district knowing that the Accused Instrumentalities constitute a material part of the inventions of the '872 patent, knowing that the Accused Instrumentalities are especially made or adapted to infringe the '872 patent, and knowing that the Accused Instrumentalities are not staple articles of commerce suitable for substantial non-infringing use.

50. With knowledge of the '872 Patent, Defendants' continuing infringement of at

least claims 1-6, 11-14, 16-21, and 26-29 has been intentional and willful.

51. On information and belief, IriusRisk, S.L. has also infringed by owning, directing, and controlling IriusRisk, Inc. and thereby using IriusRisk, Inc. to engage in one or more of the infringing acts described herein on IriusRisk, S.L.'s behalf and for its benefit.

52. On information and belief, IriusRisk, Inc. and IriusRisk, S.L. jointly infringe the '872 patent by jointly owning, operating, controlling, making, using, selling, offering for sale, and importing in the United States the Accused Instrumentalities. On information and belief, IriusRisk, Inc. and IriusRisk, S.L. jointly infringe the '872 patent by acting in concert together to operate, control, make, use, sell, offer for sale, and import in the United States the Accused Instrumentalities for the mutual benefit of each other and at the direction and control of each other.

53. Defendants' acts of willful infringement have caused damage to ThreatModeler, and ThreatModeler is entitled to recover from IriusRisk the damages sustained as a result of IriusRisk's wrongful acts in an amount subject to proof at trial, but in any event not less than a reasonable royalty.

54. ThreatModeler has been and continues to be damaged by IriusRisk's infringement of the '872 Patent. ThreatModeler has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, ThreatModeler demands judgment for itself against Defendants as follows:

A. Adjudging that Defendants have independently and/or jointly infringed the '872 Patent, either literally or under the Doctrine of Equivalents.

B. Adjudging that Defendants' infringement of the '872 Patent has been willful.

C. Awarding ThreatModeler damages for Defendants' past infringement adequate to compensate ThreatModeler for the infringement, but in any event, not less than a reasonable royalty, and for any continuing or future infringement through the date such judgment is entered, including pre-judgment and post-judgment interest, costs, expenses, and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

D. A declaration that this case is exceptional under 35 U.S.C. § 285, an awarding of treble damages, and an award of ThreatModeler's reasonable attorneys' fees;

E. Injunctive relief enjoining IriusRisk, its officers, directors, employees, parents, subsidiaries, affiliates, agents, and those acting in concert with IriusRisk from further infringement of the '872 Patent; and

F. An award of such other and further relief, at law or in equity, as the Court deems just and proper.

DEMAND FOR JURY TRIAL

ThreatModeler hereby demands a jury trial on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

DATED: January 30, 2025

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

/s/ Jeffrey B. Bove

Jeffrey B. Bove (# 998)
500 Delaware Ave., Suite 720
Wilmington, DE 19801-7407
jeffrey.bove@bipc.com
Tel. (302) 552-4200
Facsimile (302) 552-4295

Attorneys for Plaintiff ThreatModeler Software Inc.

Of Counsel:

Donald L. Jackson (VA Bar 42882)
James D. Berquist (VA Bar 42150)
RIMON P.C.
8300 Greensboro Dr., Suite 500
McLean, Virginia 22102
Tel. 571-765-7700
Facsimile 208-501-8304
donald.jackson@rimonlaw.com
james.berquist@rimonlaw.com