A Comprehensive Analysis of Automated Threat Modeling Solution Company: Threat Modeler Software, Inc.

Santosh Pai [1*], & Srinivasa Rao, Kunte [2]

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid-ID: 0000-0002-5053-1673; E-Mail: g.santoshpai@gmail.com

[2] Faculty, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid-ID: 0000-0002-5062-1505; E-Mail: kuntesrk@gmail.com

Area of the Paper: Computer Science.
Type of the Paper: Case Study.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.6984759
Google Scholar Citation: IJCSBE

How to Cite this Paper:

Pai, Santosh, & Kunte, Srinivasa Rao, (2022). A Comprehensive Analysis of Automated Threat Modeling Solution Company: Threat Modeler Software, Inc. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *6*(2), 99-107. DOI: https://doi.org/10.5281/zenodo.6984759

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Crossref DOI : https://doi.org/10.47992/IJCSBE.2581.6942.0186

Paper Submission: 19/07/2022
Paper Publication: 12/08/2022

© With Authors.

This work is licensed under a Creative Commons Attribution Non-Commercial 4.0 International License subject to proper citation to the publication source of the work.
Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

A Comprehensive Analysis of Automated Threat Modeling Solution Company: Threat Modeler Software, Inc.

Santosh Pai [1*], & Srinivasa Rao, Kunte [2]

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid-ID: 0000-0002-5053-1673; E-Mail: g.santoshpai@gmail.com

[2] Faculty, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid-ID: 0000-0002-5062-1505; E-Mail: kuntesrk@gmail.com

ABSTRACT

Purpose: *Effective Security Threat modeling in an enterprise depends on the efficient tools used for modeling. The Threat modeling tool market has multiple players that provide platforms to automate the Threat modeling process in enterprises. Threat Modeler Software, Inc. is one such platform provider company. The paper aims to explore the company and its platform's features.*

Design/Methodology/Approach: *This paper explores the documentation available on Threat Modeler Software, Inc. to understand the features, working principles, and company information. Features are further explored by performing hands-on Threat modeling using the trial edition of the platform. SWOC analysis of the company is performed to analyze the factors affecting the company as a Threat modeling platform provider.*

Findings/Result: *Threat Modeler Software, Inc.'s platform has innovative features that enable automated Threat modeling. SWOC analysis has identified some of the challenges that the company has. The competitor list showed commercial and open-source competitors in the race to create Threat modeling platforms. The innovative culture of the Threat Modeler Software, Inc. must continue to provide new features making the Threat modeling experience unique.*

Originality/Value: *This paper studies Threat Modeler platform's architecture and explores important features of the platform. Capabilities of the features and their importance are studied. SWOC analysis is performed to identify factors affecting the company. A list of different threat modeling platforms is built to understand the current competitors for Threat Modeler Software, Inc.*

Paper Type: *Case Study.*

Keywords: Threat Modeler, Threat Modeler platform, Cyber Security, Security by Design, SWOC analysis.

1. INTRODUCTION :

One of the most concerning risks for an organization in the digital era is Cyber Attacks [1]. Threat Actors are evolving their techniques and progressing ahead of the industry. The use of Artificial Intelligence to create new types of attacks [2] and the unauthorized use of computing power for Crypto mining [3] are two good examples of Cyber Threat evolution. A novice hacker could purchase hacking tools from the dark net and use them to trigger attacks on organizations and individuals [4]. A typical Software Development Life Cycle has four phases. Requirement phase, Design phase, Implementation phase, and Testing phase. Security activities in the SDLC (Software Development Life Cycle) were constrained to the Testing phase [5].

A product would be designed, implemented, and tested for security flaws. Any issues found in the product requiring a change in the design would lead to restart of the SDLC. This would require a re-design of the architecture, modifying the implementation, and re-testing the use cases. The elevated cost of security tests at the end of the SDLC was a significant concern. Any change towards the end of

SDLC requires re-testing of all or most test cases. The cost is also affected by the automation level of the test cases. Manual test cases cost additional time and money [6]. Enterprises started to comprehend the necessity of shifting security activities such as design reviews, static code analysis, and capturing the risks. Microsoft has a well-defined Secure Development Lifecycle [7] and has provided tools to realize Threat modeling. Google has launched Security by Design programs for Android application developers [8]. Amazon Web Service, a pioneer in public cloud services, has defined a shared security model for its various services and has recommended security controls for securing the cloud services [9]. Threat modeling captures security and privacy risks during a software system's design phase and suggests mitigations to be implemented. Threat Modeler Software, Inc. created an automated Threat modeling framework based on V.A.S.T methodology (Visual, Agile, Simple Threat modeling) [10] for threat modeling.

2. REVIEW OF LITERATURE :

Threat modeling tools are essential for organizations having multiple verticals of products. Available literature is collected using Google Scholar on the articles published between years 2018 to 2022. Keywords 'Threat Modeler', 'Threat Modeler' are used to perform searches. Articles are further filtered by considering discussions about the Threat Modeler platform. Details of the literature review are listed in the Table 1.

Table 1: Contribution to study of Threat Modeler platform

S. No	Field of Study	Focus	Outcomes	Reference
1.	IoT Threat Modeling	Threat modeling of IoT smart home use-cases using the Threat Modeler platform.	Threat modeler uses process flow diagrams to create architecture models. The platform identifies process-level threats. Components in the platform are more systematic compared to other Threat modeling platforms. V.A.S.T methodology for threat detection performs an in-depth analysis of the system under design.	Abbas, S. G., et al. (2020). [11]
2.	Interoperability and Security	Industrial system Threat modeling	Threat Modeler platform has a threat library and threat engine. The platform has advanced reporting capabilities.	Boniface, M., et al. (2020). [12]
3.	Threat Modeling	Architecture model derivation for Threat modeling	Threat modeler uses Process flow diagrams to illustrate the flow of assets or data in the system.	Van Landuyt, D., et al. (2021). [13]
4.	Threat Modeling Platform	Emergency Health data communication	The platform does not consider other factors such as incorrect use of the system or user behavior.	Surridge, M., et al. (2019). [14]
5.	Threat Modeling Platform	Critical System security risk assessment	Threat Modeler platform uses V.A.S.T based threat detection logic. The platform is focused on web application security assessments.	Schiavone, E., et al. (2021). [15]

3. RESEARCH GAP :

Current studies on the Threat Modeler Software, Inc. Company and its platform are at a high level. Factors affecting the company are not considered in the previous studies. For a security focused organization, it is crucial to study in-depth about the software vendor before making purchase decisions. A company analysis of Threat Modeler Software, Inc. is necessary to guide vendor assessments.

4. RESEARCH AGENDA :

Following is the agenda for this study:

1. How does the Threat Modeler platform automate the Threat modeling process?
2. What are the strengths, weaknesses, opportunities, and challenges of Threat Modeler Software, Inc.?
3. What are the essential features of the Threat Modeler platform?
4. What are some players in the Threat modeling industry?

5. OBJECTIVES OF THE STUDY :

1. To Study of Threat Modeler platform architecture
2. To Perform SWOC analysis of Threat Modeler Software, Inc.
3. To Explore important software features of the Threat Modeler platform
4. To List different players in the Threat modeling industry

6. METHODOLOGY :

The SWOC analysis is performed using the information available on Threat Modeler Software, Inc. website and articles on the internet related to the company. The Threat modeling platform features are explored using hands-on experiments on the community edition of the software.

7. STUDY OF THREAT MODELER PLATFORM ARCHITECTURE :

7.1 The Threat modeling problem:

Traditional Threat modeling requires brainstorming virtually or physically with experts from the Engineering, Architecture, and Security teams. Using Data Flow Diagrams, the complete solution is illustrated component by component, and one of the several available Threat modeling techniques is applied [15]. The result of this process is a list of probable threats and mitigations. These are documented as defined by the organization's quality management system using one of the several available documentation tools.

This process is reiterated every time there is a change in the product design, usually at the beginning of a release. Once the Threat modeling is performed and risks are documented, the reports are stored as static documents and not updated based on evolving attack surface. This creates a gap in the risk assessments performed and the actual risks in the product [16]. Organizations close this gap by defining processes that ensure Threat modeling is conducted once for a particular duration. However, the evolving attack surface and new vulnerabilities developing daily make it inefficient to perform Threat modeling frequently during a release.

7.2 The Threat modeler solution:

Threat Modeler is an automated Threat modeling Framework for performing and managing threat models throughout a product's lifecycle designed by Threat Modeler Software, Inc.

7.3 Threat Modeler Architecture:

Threat Modeler is an Automated Threat Intelligence Framework with different components, as shown in Fig.1.

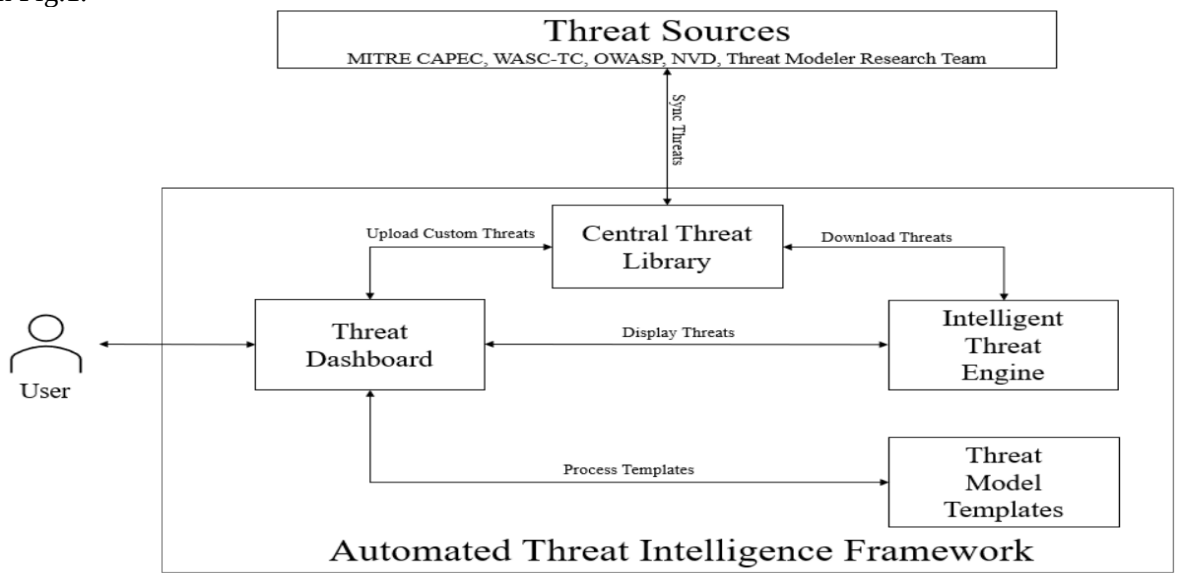

Fig.1: Threat Modeler Architecture Diagram

Threat Dashboard: It is the Graphical User Interface that helps create diagrams for the user of the software. The user interface comprises components and relations. Components are pieces of software that make workable software when combined. A Web browser is an example of a Component. A relation is a connection between components, such as TCP or HTTP or HTTPS. The user can drag and drop the components on the screen. Components are then connected using relations. Both components and relations have attributes that the user fills. The software generates the threats based on the diagram components, relations, and attributes. The threat list is updated in real-time as the diagram is updated.

Intelligent Threat Engine: It is the heart of the solution that combines the user-provided architecture of the software with the threat library and generates the threats for the software being assessed. It has the intelligence to modify the threat list and individual threats based on the software design provided and the attributes of the components.

Central Threat Library: It is a library of threats and related information built using threat sources available globally and the custom threats provided by the organization in the context of software being assessed.

Threat Model Templates: It is a library of threat models that can be re-used when assessing software. For example, banking software contains E-mail generator software as a component. The threat model template can be used to save the E-mail generator threat model, which can be later used in different banking Software such as Web-based banking, Mobile application, etc.

Threat Sources: These are external sources, not part of the Threat Modeler itself. But these sources provided the globally known threats. Threat Modeler continuously synchronizes with such sources to collect the threat data.

8. SWOC ANALYSIS :

Threat Modeler Software, Inc. was founded by Archie Agarwal in 2010 [17][18]. The initial name of the Company My App Security, Inc. was changed to the current name Threat Modeler Software, Inc. in 2018. The company was established with the vision of integrating Threat modeling in the SDLC and reducing the organization's overall risk posture. The company holds more than 15 patents [19] in the Threat modeling area, which shows the company's innovative culture. The company has won numerous information security awards [20].

SWOC analysis [29] of Threat Modeler Software, Inc. describes the Strength, Weaknesses, Opportunities, and Challenges around the Automated Threat modeling framework solution of Threat Modeler Software, Inc. It is depicted in Table 2.

Table 2: The SWOC Analysis of Threat Modeler Software, Inc

Strengths of Threat Modeler	❖ Automation capabilities to keep the Threat model up to date with new threats from different sources ❖ Cloud-based software stack allows easy access from anywhere without geographical boundaries. ❖ Collaboration between stakeholders is a mandatory requirement for Threat modeling. This is enabled by the cloud hosted platform. ❖ Exhaustive components enable creating technically detailed software architecture diagrams ❖ The company has patented several innovative features, making them exclusively available on their platform ❖ The Threat model chaining allows aggregation of previously developed threat models

	❖ The Threat model template enables creating of custom complex components and using them in the software architecture diagrams.
Weakness of Threat Modeler	❖ Creating the diagrams for Threat modeling is time consuming process ❖ False-positive threats generated by the platform adds delay, as it requires user intervention ❖ For a new user, it takes significant time to read help pages, watch videos, and read blogs before exploring all features. ❖ The Community Edition is available for 30 days. The time is sufficient to explore the tool. However, minimal features are provided.
Opportunities of Threat Modeler	❖ Threat modeling can play a crucial role in DevSecOps to automate the Threat modeling process, left shifting the security design process & saving the cost. ❖ Threat modeling also has scope in the maintenance of the product post-deployment. New vulnerabilities and security issues impacting the deployed products can be expected and mitigated without manually maintaining the product's security posture.
Challenges of Threat Modeler	❖ The Graphical User Interface experience is average, and user interface improvement is required to make it easy for the users to draw diagrams. ❖ Justifying the cost of automation of Threat Modeler against the other available freeware and open source Threat modeling tools is a challenge. The other tools, such as OWASP Threat Dragon [21][22] and Threagile [21][23], provide options to create fully automated Threat modeling for Agile teams. ❖ The delay in loading the web-based graphical user interface impacts usability

9. FEATURE EVALUATION :

As part of the Threat Modeler exploration, we performed a hands-on evaluation of the features. Feature documented on the company website are explored using the community edition of the Threat Modeler platform. Evaluation details are listed in Table 3.

Table 3: List of Threat Modeler platform features evaluated

S. No	Feature Title & Description	Evaluation Comments	Reference
1.	**The Intelligent Threat Engine (ITE)** ITE is the brain of the platform. It generates threats for every component in the system architecture. The threats are sourced from a threat library.	Multiple threats are generated for every component as soon as they are added to the diagram. Each threat is also associated with corresponding mitigation.	[24]
2.	**Diagramming Tool** The feature enables drawing Process Flow Diagrams in the Threat Modeler platform using system components.	The drawing interface is a familiar drag and drop-based user interface. Using the mouse makes it possible to draw complex data flow diagrams.	[25]
3.	**Component Toolbox**	In the Community edition, there are around 400 components available. The	[24][26][27]

	Components are the building blocks of the Process Flow Diagrams. The Threat Modeler platform has more than 1000 components.	list has generic processes such as Login, Graphical User Interface, Authentication, etc. It also has Specific Processes such as AWS Lambda, VMWare Components, etc. These processes are labeled for easy searching.	

10. COMPETITORS :

Threat Modeler Software, Inc. has several competitor products in open-source and commercial categories [21], [28]. Table 4 below lists some of the competitors.

Table 4: List of other Threat modeling Tools

S. No	Name of the Product	License Type	Owner OR Contributor
1.	Microsoft Threat Modeling Tool	Freeware	Microsoft
2.	OWASP Threat Dragon	Opensource	Community Contributed
3.	OWASP pytm	Opensource	Community Contributed
4.	Threagile	Opensource	Community Contributed
5.	CAIRIS	Opensource	Community Contributed
6.	Threatspec	Opensource	Community Contributed
7.	IriusRisk	Commercial	IriusRisk
8.	securiCAD Professional	Commercial	Foreseeti
9.	SD Elements	Commercial	Security Compass
10.	Kenna	Commercial	Kenna Security
11.	Tutamen Threat Model Automator	Commercial	Tutamantic Sec

11. FINDINGS :

This section lists the findings of the research.
1. The Threat Modeler platform is available as cloud software.
2. Diagramming utility built in the software allows users to draw complex architectures.
3. Use of the platform does not require installation of custom software on user's computer.
4. Threat model templates enable re-use of the Threat models created across organizations.
5. Model Chaining feature allows including existing Threat models in new projects.
6. Exhaustive list of components allows users to create detailed architecture diagrams.
7. Threat Modeler Software, Inc. holds several patents for innovative features of the platform.
8. A community edition of the software is provided for trial purpose to explore the features.
9. There are more than ten Threat modeling tools available in the market including open source and licensed software.

12. SUGGESTIONS :

Based on this study, we have below suggestions.
1. Automation of threat modeling is a necessary feature to be considered for organizations creating enterprise software having complex architectures.
2. User interface of the platform requires improvements to provide usability for the model creator.
3. Community edition of the software to be explored before purchasing the full license for the software.
4. Innovative culture of Threat Modeler Software, Inc. must continue to add more innovations in their products.
5. Provide offline version of the software to create Threat models without connecting to internet, especially in case of remote working.

13. SUMMARY AND CONCLUSION :

The Threat Modeler framework has innovative features that make it a suitable solution for automating the threat generation process. Being a cloud-based solution, it allows collaborative Threat modeling for

enterprises. We studied the features of the Threat Modeler based on the documentation available on the company's website. Using the Community Edition of the platform, we explored some of the features, and they are found to be fully implemented in the platform. The framework has innovative features such as an Intelligent Threat Engine and Threat model Chaining. It proves to be a good choice for creating live and automated threat models. There is an opportunity for improvement in the framework's usability by providing on-screen help and demo mode options. It is also evident that many open source and commercial Threat modeling platforms exist. Our future work includes researching other Threat modeling tools and their automation capabilities.

14. ACKNOWLEDGEMENTS :

Threat Modeler Software, Inc. provides a Community Edition of the platform for users to explore features. This edition is available for thirty days as a Software as a Service model. The community edition allows the creation of one threat model, and some of the platform's features are available. We thank Threat Modeler Software, Inc. for providing the community edition of the platform. In this paper, the evaluation of the features is done using the community edition.

REFERENCES :

[1] Chernyakov, M., & Chernyakova, M. (2018). Technological Risks of the Digital Economy. *Journal of Corporate Finance Research / Корпоративные Финансы*, *12*(4), 99–109. Google Scholar↗ CrossRef/DOI↗

[2] Brundage, M. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Accessed on 28/01/2022. Google Scholar↗

[3] Sigler, K. (2018). Crypto-jacking: How cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), 12–14. Google Scholar↗ CrossRef/DOI↗

[4] Ollmann, G. (2008). Hacking as a service. *Computer Fraud & Security*, *2008*(12), 12–15. Google Scholar↗ CrossRef/DOI↗

[5] Nazir, N., & Nazir, M. K. (2018). A review of security issues in SDLC. *American Academic Scientific Research Journal for Engineering, Technology, and Sciences*, *46*(1), 247-259. Google Scholar↗

[6] Kumar, D., & Mishra, K. K. (2016). The impacts of test automation on software's cost, quality, and time to market. *Procedia Computer Science*, *79*(1), 8–15. Google Scholar↗ CrossRef/DOI↗

[7] Lipner, S. (2010). Security development lifecycle. *Datenschutz Und Datensicherheit - DuD*, *34*(3), 135–137. Google Scholar↗ CrossRef/DOI↗

[8] Introducing Security by Design. Google Online Security Blog. https://security.googleblog.com/2021/05/introducing-security-by-design.html. Accessed on 21/01/2022.

[9] Security by Design - Amazon Web Services (AWS). (2015). Amazon Web Services, Inc. https://aws.amazon.com/compliance/security-by-design/. Accessed on 28/01/2022.

[10] Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

https://apps.dtic.mil/sti/citations/AD1084024.Accessed on 28/01/2022.

[11] Abbas, S. G., Zahid, S., Hussain, F. Shah, G. A. and M. Husnain (2020). A Threat Modelling Approach to Analyze and Mitigate Botnet Attacks in Smart Home Use Case.*2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, 122-129. Google Scholar↗ CrossRef/DOI↗

[12] Boniface, M., Fair, N., Modafferi, S., & Papay, J. (2020). Security Implications of Interoperability. *In Proceedings of the Workshops of I-ESA 2020*(1-5). Google Scholar↗

[13] Van Landuyt, D., Pasquale, L., Sion, L. and Joosen, W. (2021). Threat modeling at run time: the case for reflective and adaptive threat management (NIER track). 2021 International Symposium on

Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 203-209. Google Scholar↗ CrossRef/DOI↗

[14] Surridge, M. et al. (2019). Modelling Compliance Threats and Security Analysis of Cross Border Health Data Exchange. In Springer's New Trends in Model and Data Engineering. *Communications in Computer and Information Science, 1085(1),* 180-189. CrossRef/DOI↗

[15] Schiavone, E., Nostro, N., & Brancati, F. (2021). A MDE Tool for Security Risk Assessment of Enterprises. In *Anais Estendidos do X Latin-American Symposium on Dependable Computing*, 5-7. Google Scholar↗ CrossRef/DOI↗

[16] Cruzes, D. S., Jaatun, M. G., Bernsmed, K., & Tøndel, I. A. (2018). Challenges and experiences with applying microsoft threat modeling in agile development projects. *In 2018 25th Australasian Software Engineering Conference (ASWEC)*, 111-120. IEEE. Google Scholar↗ CrossRef/DOI↗

[17] Forbes. (2019). Archie Agarwal. Forbes Councils.https://profiles.forbes.com/members/tech/profile/Archie-Agarwal-Founder-CEO-%7C-Chief-Technical-Architect-ThreatModeler-Software-Inc/892981db-9517-4101-a549-8535d69e0cd2. Accessed on 28/01/2022.

[18] Threat Modeler Software, Inc. (2019, August 28). About Us. Threat Modeler Software, Inc. .https://threatmodeler.com/about/.Accessed on 28/01/2022.

[19] Patents Assigned to Threat Modeler Software Inc. - Justia Patents Search. (2022). Justia. https://patents.justia.com/assignee/threatmodeler-software-inc.Accessed on 28/01/2022.

[20] Threat Modeler Software, Inc Wins Two Categories by Global Infosec Awards for 2021. (2021). News Direct. https://newsdirect.com/news/threatmodeler-software-inc-wins-two-categories-by-global-infosec-awards-for-2021-779437638?category=Real%20Estate. Accessed on 28/01/2022.

[21] Shi, Z., Graffi, K., Starobinski, D., & Matyunin, N. (2021). Threat Modeling Tools: A Taxonomy. *IEEE Security & Privacy*, Advance online publication. Google Scholar↗ CrossRef/DOI↗

[22] Bygdås, E., Jaatun, L. A., Antonsen, S. B., Ringen, A., & Eiring, E. (2021). Evaluating threat modeling tools: Microsoft TMT versus OWASP Threat Dragon. *In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-7. IEEE. Google Scholar↗ CrossRef/DOI↗

[23] Threagile, Agile Threat Modeling. https://threagile.io/. Accessed on 26/03/2022.

[24] Threat Modeler Software, Inc. (2020, January 1). THREATMODELER FEATURES. https://threatmodeler.com/threatmodeler/. Accessed on 26/03/2022.

[25] Threat Modeler Software, Inc. (2020, January 22). ARCHITECTURALLY BASED PROCESS FLOW DIAGRAMS: EXAMPLES AND TIPS TO FOLLOW. https://threatmodeler.com/architecturally-based-process-flow-diagrams/. Accessed on 26/03/2022.

[26] Amazon Web Services, Inc. (2021, October 20). AWS Serverless Multi-Tier Architectures with Amazon API Gateway and AWS Lambda. https://docs.aws.amazon.com/whitepapers/latest/serverless-multi-tier-architectures-api-gateway-lambda/serverless-multi-tier-architectures-api-gateway-lambda.pdf. Accessed on 26/03/2022.

[27] Threat Modeler Software, Inc. (2020, April 28). Threat Modeler launches, free lite community edition. https://threatmodeler.com/threatmodeler-launches-free-lite-community-edition/. Accessed on 26/03/2022.

[28] Schaad, A., & Reski, T. (2019). Open Weakness and Vulnerability Modeler (OVVL)–An Updated Approach to Threat Modeling. *In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications – SECRYPT*, 417-424. Google Scholar↗ CrossRef/DOI↗

[29] Aithal, P. S., & Kumar, P. M. (2015). Applying SWOC analysis to an institution of higher education. *International Journal of Management, IT and Engineering*, *5*(7), 231-247. Google Scholar↗