A Review of Asset-Centric Threat Modelling Approaches

Livinus Obiora Nweke[1]
Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

Stephen D. Wolthusen[2]
School of Mathematics and Information Security
Royal Holloway, University of London
Egham, United Kingdom
Information Security and Communication Technology
Norwegian University of Science and Technology (NTNU)
Gjøvik, Norway

***Abstract*—The threat landscape is constantly evolving. As attackers continue to evolve and seek better methods of compromising a system; in the same way, defenders continue to evolve and seek better methods of protecting a system. Threats are events that could cause harm to the confidentiality, integrity, or availability of information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information system. The process of developing and applying a representation of those threats, to understand the possibility of the threats being realized is referred to as threat modelling. Threat modelling approaches provide defenders with a tool to characterize potential threats systematically. They include the prioritization of threats and mitigation based on probabilities of the threats being realized, the business impacts and the cost of countermeasures. In this paper, we provide a review of asset-centric threat modelling approaches. These are threat modelling techniques that focus on the assets of the system being threat modelled. First, we discuss the most widely used asset-centric threat modelling approaches. Then, we present a gap analysis of these methods. Finally, we examine the features of asset-centric threat modelling approaches with a discussion on their similarities and differences.**

***Keywords*—Threat modelling; asset-centric; asset-centric threat modelling approaches**

I. Introduction

Threats are events that could cause harm to the confidentiality, integrity, or availability (CIA model [1]) of information systems, through unauthorized disclosure, misuse, alteration, or destruction of information or information system [2]. The process of developing and applying a representation of those threats, to understand the possibility of the threats being realized is referred to as threat modelling. It includes selecting a threat modelling framework and populating that framework with specific values (e.g. adversary expertise, attack patterns and attack events) as relevant to the intended scope (e.g. architectural layers or stakeholder concerns). The populated framework can then be used to construct threat scenarios; characterize controls, technologies, or research efforts; and/to share threat information and responses [3].

Threat modelling methodologies are very few; although there are several frameworks or threat classification models that are usually combined and leveraged by threat modelling methodologies [4]. The choice of threat modelling approach to adopt for a particular situation is dependent on the business objectives. It follows that the first step towards choosing the threat modelling technique to use for a system is to have a clear understanding of what the system being threat modelled is supposed to do. Basically, there are no good or bad threat modelling methods but rather, there are good and bad threat modelling approaches for a particular system.

There are three main approaches that are usually deployed for threat modelling activities and they include: the approaches that focus on the assets of the system being threat modelled, which are referred to as asset-centric threat modelling approaches; the approaches that focus on the attackers, also called the attack-centric threat modelling approaches; and the approaches that focus on the software or the system, which are referred to as software-centric or system-centric threat modelling approaches [5]. We are mainly concern with the asset-centric threat modelling approaches in this paper.

In this paper, we provide a review of asset-centric threat modelling approaches. First, we examine the general objectives and benefits of threat modelling. Also, we present a discussion on the existing threat modelling approaches and justification for reviewing asset-centric threat modelling approaches. We observe that DREAD (damage, reproducibility, exploitability, affected users, discoverability), Trike, OCTAVE (operationally threat asset, and vulnerability evaluation) and PASTA (process for attack simulation and threat analysis) are the most widely used asset-centric threat modelling approaches. The limitation of these approaches is presented. We also examine the features of the asset-centric threat modelling approaches. And using these features, we present a discussion on their similarities and differences. The overall goal of this review is to serve as a foundation for selecting asset-centric threat modelling approaches and to further advance the use of asset-centric methodologies in threat modelling activities.

The rest of this paper is organised as follows. Section II examines the general objectives and benefits of threat modelling. Also, a discussion on the existing threat modelling approaches is presented with the justification for reviewing asset-centric threat modelling approaches. Section III presents state-of-the-art of the most widely used asset-centric threat modelling approaches. Section IV presents gap analysis of the asset-centric threat modelling approaches reviewed. Section V discusses the similarities and differences of the asset-centric threat modelling approaches based on their features. Section

VI concludes the paper and present future work.

II. Background

In this section, we examine the general objectives and benefits of threat modelling. We also present a discussion on the existing threat modelling approaches and justification for reviewing the state-of-the art in the asset-centric threat modelling approaches in this paper.

A. Threat Modelling

Threat modelling is a systematic approach for characterizing potential threats to a system. It ensures completeness by including the prioritization of threats and mitigation based on probabilities, business impacts and cost of countermeasures. Threat modelling provides a means of evaluating all possible risks throughout the system and not just concentrating on where flaws are expected to be discovered [6]. It is also useful in ranking the likelihood of a threat being realized. An essential step for threat modelling is having an understanding of assets and threats [4].

Assets are usually discrete data entities, but they can be physical objects, which feature in the business rules of a system [6]. Assets are artefacts which are important to a specific problem domain of a system, and not just in the actual implementation of a system. Identifying assets can be a very challenging endeavour, but it is the initial step that needs to be carried out in order to understand the amount of resource which can be allocated for threat modelling activities. Also, the amount of threats increases geometrically as the number of assets increases [6].

UcedaVelez and Morana [4] observe that most organizations, businesses, and governments depend on sources such as threat intelligence for the acquisition of threat knowledge. It is obvious that threats would mean different things to different types of organizations. For instance, in the case of private organization, potential threats are those targeting their business assets. For government organizations, potential threats are those relating to national security. Analysing the potential threat scenarios that target an organization's assets is important in determining the likelihood of the threats being realized.

Once the analysis of the potential threat scenarios has been concluded and it shows that the system being threat modelled is at risk, the next step of the risk mitigation strategy is to determine if similar assets are also exposed and can be affected [4]. Also, it is important to consider whether the mitigation measures suggested are able to eliminate the risk to the system without creating additional security threats. This ensures a wholistic mitigation measures are adopted to reduce the business impact of the threat being realized.

Another important factor to consider during threat modelling is the business impact of a threat being realized. A business impact is different from information security risk in that it measures the economic impact caused by either the loss or the compromise of an asset while information security risk affects the confidentiality, integrity and availability of data [4]. Determining the business impact requires a consideration for the business context in which the system operates. This can be achieved by examining at a high level, the assets of the system and the functionality the system provides based on these assets.

In general, threat modelling involves a great amount of effort and resources of so many individuals beyond those of information security [4]. It encourages collaboration and as such, the threat modelling methodology that should be deployed for a particular system may have to consider how collaboration can be fostered. The next subsection presents the different threat modelling approaches. We agree with the authors in [4] that none of these approaches are flawed but rather the way in which they are selected may be flawed.

B. Threat Modelling Approaches

Threat modelling approaches can be categorized according to the focus of the approaches. These approaches include those that focus on the assets of the system being threat modelled, which are referred to as asset-centric threat modelling approaches; the approaches that focus on the attackers, also called attack-centric threat modelling approaches; and the approaches that focus on the software or the system, which are referred to as software-centric or system-centric threat modelling approaches [5]. Deciding which of the method to deploy depends on the system being threat modelled and the tools available.

Asset-centric threat modelling approaches focus on the assets of the system being threat modelled. It involves analysing the information loss or business impact of targeted assets. Asset-centric threat modelling can be extended beyond identifying the motives and intentions of the attacker to incorporating the discovery of security gaps for the system environment [4]. Although, asset-centric threat modelling is not concerned about flaws or insecure coding/design practices, it could be used to uncover possible threats scenarios.

Attack-centric threat modelling approaches include those approaches that focus on the attacker. The idea here is to examine the threats against a system from the perspective of an attacker. Attack-centric threat modelling approach aims to identify which threats can be successfully executed against a system given a number of identified misuse cases, vulnerabilities, and more [4]. Also, the approach attempts to examine the motive, sources and relative identity of the attacker or group associated with the attacker as these can help to uncover the approach and resources of the attacker [4].

System-centric threat modelling approaches focus on the system being threat modelled. They first consider the design model of the system under consideration. The objective of these approaches is to ensure that the complexity of the system being threat modelled is well understood before considering threats the system may be exposed to. System-centric threat modelling approaches expects those involved in threat modelling of a system, to have a good grasp of the system they are developing [5].

In this paper, we interested in understanding the state-of-the-art in asset-centric threat modelling approaches. It is usually the case that most businesses have a clear understanding of their business objectives and assets to be protected. Also, the system to be threat modelled and the business impacts of threats being realized are likely to be known. Thus, the obvious threat modelling approaches that can be employed for the protection of assets, understanding and managing business risks for most businesses are the asset-centric threat modelling

approaches. Therefore, we present this review to serve as a basis for selecting or combining the appropriate asset-centric threat modelling approaches and to further advance the use of asset-centric threat modelling techniques.

III. The State-of-the-Art in Asset-Centric Threat Modelling Approaches

In this section, we present a review of asset-centric threat modelling approaches. We observe that the most widely used asset-centric threat modelling approaches are DREAD, Trike, OCTAVE, and PASTA. We use this understanding to present a discussion on the state-of-the-art in asset-centric threat modelling approaches.

A. DREAD

DREAD is an acronym for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. It is an asset-centric threat modelling approach developed by Microsoft. DREAD uses the traditional qualitative risk rating (HIGH, MEDIUM, LOW) with a qualitative risk rating 3,2,1 applied respectively. In general, DREAD threat modelling approach uses a scoring system to calculate the probability of occurrence for each of the identified areas of the asset being threat modelled. By combining the risk rating values obtained, DREAD threat modelling approach is able to predict the probability of occurrence of each threat identified during the threat modelling process [4].

The Damage potential refers to the level of havoc that could be done to users and the organization if an attack were to succeed. Damage could be concrete, such as financial liability or abstract, such as damage to organization's reputation. Also, it depends on the nature of the attack and the assets being targeted. Reproducibility measures the easy with which the attack can be replicated. The goal is to measure the effort that would be expended by an attacker for the realization of an attack and use such measure, in the scoring system. If an attack can be reproduced with much ease, the attack would be rated high in the scoring system as against an attack that cannot be reproduced with much ease.

The remaining letters of DREAD are described as follows. Exploitability describes the possibility of an attacker taking advantage of a vulnerability. Several exploits exist and they can be classified as those that are easily understood and could be accomplished by anyone and those that are difficult that required specialized skills to achieve. This understanding is used to rate threat that have high level of exploitability as high risk in the scoring system and those with low level of exploitability as low risk. Affected users refers to the number of users that will be affected by the realization of a particular threat. A threat that is likely to affect a great number of users when realized would have a higher risk factor rating compared to a threat that is likely to affect a limited number of users. Discoverability describes the ease with which the vulnerability is uncovered. There are threat that are very difficult to learn and those that can be learn with ease. Hence, a threat that is very difficult to learn would be rated lower than those that has been released in the public domain. The DREAD approach is summarised in Fig. 1.

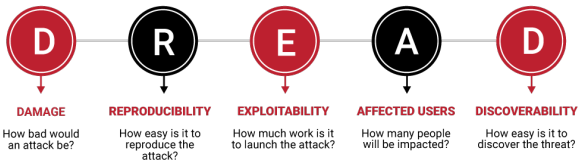

Fig. 1. DREAD Summary [7]

Although DREAD is an asset-centric threat modelling approach, several of its application in the literature is in combination with STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) model [8], [9], [10], [11], [12]. In this type of approach, the DREAD scoring scheme is used to identify the likelihood that an attack is able to exploit a particular threat.

B. Trike

Trike offers a threat modelling approach which is asset-centric and it achieves that through the generation of threat models in a reliable, and repeatable manner [6]. It facilitates constructive interaction among relevant stakeholders by providing standardized framework for reasoning about threats that a system would have to overcome. The achievement of Trike objectives entail the following [6]:

- With assistance from the system stakeholders, ensure that the risk the system presents to each asset is acceptable to all stakeholders.
- Be able to tell whether that have been done.
- Communicate what have been done and it effects to the stakeholders.
- Empower stakeholders to understand and reduce the risks to themselves and other stakeholders implied by their actions within their domains.

Another important observation about Trike is that it follows a defensive approach. Understanding the system itself and the environment in which the system is going to be used is more important when using Trike threat modelling approach than understanding the capability of an attacker. This is because without a complete knowledge of the system, it is difficult to appropriately characterize the threat that a system would have to face [6].

C. OCTAVE

OCTAVE is another asset-centric threat modelling approach. It is an acronym for Operationally Threat Asset, and Vulnerability Evaluation. OCTAVE methodology takes the advantage of people's understanding of their organization's security-related practices and process to model the state-of-the-art of security practice within the organization. Threat to the most critical assets are used to prioritize areas of improvement and to set security strategy for the organization [13].

The two aspects that are the foundation of OCTAVE approach include: operational risk and security practices. The security practices encompasses efforts by an organization to refine its existing security practices. Technologies deployed by an organization in meeting its business objectives are evaluated in relation to security practices. For the operational risks, an organization considers all aspects of risk (asset, threats, vulnerabilities, and organization impact) in its decision making enabling the organization to match a practice-based protection strategy to its security risks [13]. The OCTAVE process is depicted in Fig. 2.

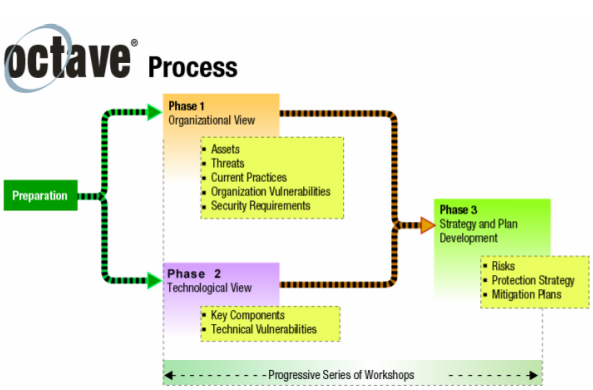

Fig. 2. OCTAVE Process [13]

The evaluation process of OCTAVE approach involves the following [13]:

- Identify information-related assets that are important to the organization;
- focus risk analysis activities on those assets judged to be most critical to the organization;
- consider the relationships among critical assets, the threat to those assets, and vulnerabilities (both organization and technological) that can expose assets to threats;
- evaluate risks in an operational context, i.e. how they are used to conduct an organization's business and how those assets are at risk due to security threats;
- create a practice-base protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization's critical assets.

In addition, the evaluation process for the organizational, technological, and analysis aspects are complemented by a three-phased approach, namely build asset-based threat profiles; identify infrastructure vulnerabilities, and develop security strategy and plans [13].

It is also imperative to note that the essential elements or requirements of the OCTAVE approach are captures in a set of criteria [13]. As of now, there are three methods consistent with the criteria and they are: the OCTAVE Method, that is designed for large organization; the OCTAVE-S, which is well-suited for small organizations; and the most recent version called the OCTAVE Allegro. The OCTAVE Allegro has been applied in [14] to evaluate the security risks of IoT (Internet of things) based smart homes. The authors in [15] developed a university information security risk management framework using OCTAVE Method based on ISO/EIC 27001:2013. Also, the OCTAVE-S has been combined with ISO 27001:2005 in [16] for risk management.

D. PASTA

PASTA is an acronym for Process for Attack Simulation and Threat Analysis which is an asset-centric threat modelling approach. It combines topicality, substantiation, and probabilistic analysis as the key three attributes as part of its methodology [4]. According to UcedaVelez and Morana [4], PASTA approach can be deployed in almost any scenario except for those scenarios where executive sponsorship of its process and produced artefacts is not available. This is because the deliverables produced by the PASTA approach are supposed to be familiarized with the organization's executives too.

When adopting and executing PASTA threat modelling approach, it is essential to review the following: sponsorship and support (without executive support the process will not succeed); maturity, as the maturity of the processes and controls employed will affect the outcome of PASTA; awareness, efficient and effective communication is required for the entire activities; input and outputs, people are the main input to consider for the threat modelling activity and outputs are to be defined for each process involved in the threat modelling; and lastly participants are recruited and retrain [4].

For the actual deployment, the PASTA threat modelling methodology include the following stages. The first stage involves defining objectives, where the business objectives of the system to be threat modelled is clearly defined. The technological scope is defined in the second stage and it involves identifying all the assets of the system. Next, the system is decomposed to facilitate an understanding of the system's operations. In the fourth stage, threat analysis is carried out to identify threats to the system. Then, weakness and vulnerability analysis which allows vulnerable areas across the system to be identified and mapped to the attack tree introduced in the threat analysis stage. Attack modelling and simulation is followed and the focus is to study the possibility that the identified vulnerabilities can be exploited. Lastly, residual risk analysis and management is done to mitigate threat that are major concerns to the system. All these stages are shown in Fig. 3.

IV. Limitation of the Asset-Centric Threat Modelling Approaches

In this section, we present a gap analysis of the asset-centric threat modelling approaches discussed in Section III.

1) DREAD: has been shown to be fairly subjective and leads to inconsistent results [3]. In fact, as of 2010, Microsoft discontinued the use of DREAD for their software development life-cycle [3]. This further underscores the limitation of DREAD as a threat modelling approach. However, DREAD is still widely used and recommended for threat and risk modelling endeavours. Hence, useful suggestions have been made in [17] on modifications to the scoring scheme in order to improve its reproducibility.

Fig. 3. PASTA Stages [4]

2) Trike: requires an analyst undertaking a threat modelling exercise to have full a grasp of the whole system while assessing the risk of attacks. This can be very challenging if the system to be threat modelled is very large. Also, the authors in [18] observed that the Trike scoring system is too vague to represent a formal. In addition, Trike does not have sufficient documentation even though its website is still available.

3) OCTAVE: is a robust, asset-centric threat modelling approach but it is highly complex. It takes considerable time to learn and the processes involved can be time consuming. Also, OCTAVE documentation can become voluminous, which is likely to discourage policy makers from adopting it as a threat modelling approach for their organization.

Another limitation of OCTAVE threat modelling approach is the way in which the identification and classification of threat is achieved. The capturing of risks and threats using the threat tree when OCTAVE is employed can become undesirable for complex environment. As the number of paths increases in the case of a very large computing environment, it may become unclear which of the paths represent the threats being modelled.

4) PASTA: is design for organizations that desire to position threat modelling with their strategic objectives. This is because PASTA incorporates business impact analysis as an important part of the PASTA process, which extends security responsibilities to the entire organization. This positioning can become a drawback for using PASTA because it may require several hours of training and education of the key stakeholders.

V. Discussion

This section presents a discussion on the similarities and differences of the asset-centric threat modelling approaches we have presented so far. First, the features of the asset-centric threat modelling approaches are given in Table I. We then provide a discussion on their similarities and differences.

A feature that is common to all the asset-centric threat modelling approaches as can be observed from Table I, is the fact that they all contribute to risk management process. In fact, asset-centric threat modelling approaches are sometimes referred to as risk-based threat modelling approaches [4]. They employ a risk-based approach in analysing the business impact of possible threat scenarios. This can then be used to prioritize threat mitigation strategies, which is also a feature that all the asset-centric threat modelling approaches we have presented in this paper possesses.

Apart from DREAD, the remaining asset-centric threat modelling approaches encourage collaboration among the stakeholders and can be used to identify relevant mitigation techniques. Collaboration is an essential part of any threat modelling activities. Considering that majority of the asset-centric threat modelling approaches presented in this review encourage collaboration among relevant stakeholders further buttress the importance of collaboration during threat modelling process. Mitigation techniques ensures that actionable steps which can help to avoid the threats identified during the threat modelling process are recommended.

Another important desirable characteristics of any threat modelling approach are reproducibility and automation. Reproducibility refers to the ability of the threat modelling approach to have consistent results when repeated. Unfortunately, the only asset-centric threat modelling approach that seems to have such property is OCTAVE. Other approaches are usually subjective and depend on those carrying out the threat modelling activities. Automation ensures that the threat modelling process can be undertaken without human intervention. As of now, only Trike has automated components and given the insufficient documentation there is still a lot of work to be done in automating asset-centric threat modelling approaches.

VI. Conclusion

Asset-centric threat modelling approaches have shown to be effective for the protection of assets, understanding and managing business risks. In this paper, we have reviewed the state-of-the-art in asset-centric threat modelling approaches. We have observed that DREAD, Trike, OCTAVE, and PASTA are the most widely used asset-centric threat modelling approaches. Then, we present a discussion on the state-of-the-art of these approaches. Also, a gap analysis of these approaches is discussed. Finally, we describe the features of the asset-centric threat modelling approaches we have reviewed, with a discussion on their similarities and differences.

In the future, we hope to explore formal methods that can exploit asset-centric threat modelling approach to reason about the potential threats to a cyber-physical system. This is because the asset-centric threat modelling approaches we have reviewed in this paper are not suitable for capturing the potential threats to a cyber-physical system due to the timing, uncertainty, and dependencies that exist between its entities. Although, several attempts have been made in the literature to threat model cyber-physical systems [19], [20], [21], we intend to use the formal method for expressing the requirements that are unique to a

TABLE I. FEATURES OF ASSET-CENTRIC THREAT MODELLING APPROACHES

Asset-centric Threat Modelling Approach	Features
DREAD	• Helps to assess risk associated with a threat exploit • Can predict the probability of an exploit being realized • Contributes to risk management • Has built-in prioritization of threat mitigation • Offers flexibility and can be applied and adopted to any situation
Trike	• Encourages collaboration among stakeholders • Has built-in prioritization of threat mitigation • Has automated components • Contributes to risk management • Can identify mitigation techniques
OCTAVE	• Encourages collaboration among stakeholders • Has built-in prioritization of threat mitigation • Has consistent results when repeated • It is designed to be scalable • Contributes to risk management • Can identify mitigation techniques
PASTA	• Encourages collaboration among stakeholders • Has built-in prioritization of threat mitigation • Contributes to risk management • Can identify mitigation techniques.

cyber-physical system in order to facilitate the identification of potential threats to the system.

REFERENCES

[1] L. O. Nweke, "Using the cia and aaa models to explain cybersecurity activies," *PM World Journal*, vol. 6, 2017.

[2] NIST, "Information security: Guide for conducting risk assessments," Sep. 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[3] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber threat modeling: Survey, assessment, and representative framework," The Homeland Security Systems Engineering and Development Institute, Tech. Rep., 2018.

[4] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, May 2015.

[5] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, Feb. 2014.

[6] M. Eddington, B. Larcom, and E. Saitta, "Trike v1 methodology document," 2005.

[7] Wildcard, "Threat modeling." [Online]. Available: https://wildcardcorp.com/security/threat-modeling

[8] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *Proc. IEEE Wireless Communications and Networking Conf. Workshops (WCNCW)*, Apr. 2018, pp. 314–319.

[9] A. Omotosho, B. A. Haruna, and O. M. Olaniyi, "Threat modeling of internet of things health devices," *Journal of Applied Security Research*, vol. 14, pp. 106–121, 2019.

[10] A. Amini, N. Jamil, A. R. Ahmad, and M. R. Z'aba, "Threat modeling approaches for securing cloud computin," *Journal of Applied Sciences*, vol. 15, pp. 953–967, 2015.

[11] M. Abomhara, M. Gerdes, and G. M. Køien, "A stride-based threat model for telehealth systems," *Norsk informasjonssikkerhetskonferanse (NISK)*, vol. 8, no. 1, pp. 82–96, 2015.

[12] M. Hagan, F. Siddiqui, and S. Sezer, "Policy-based security modelling and enforcement approach for emerging embedded architectures," in *Proc. 31st IEEE Int. System-on-Chip Conf. (SOCC)*, Sep. 2018, pp. 84–89.

[13] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," 2003.

[14] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for iot-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 3 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/3/817

[15] I. Sulistyowati and R. H. Ginardi, "Information security risk management with octave method and iso/eic 27001: 2013 (case study: Airlangga university)," *IPTEK Journal of Proceedings Series*, no. 1, pp. 32–38, 2019.

[16] S. Stephanus, "Implementation octave-s and iso 27001controls in risk management information systems," *ComTech: Computer, Mathematics and Engineering Applications*, vol. 5, no. 2, p. 685, 2014.

[17] D. Leblanc, "Dreadful," 2007. [Online]. Available: https://blogs.msdn.microsoft.com/david-leblanc/2007/08/14/dreadful/

[18] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," *no. July*, 2018.

[19] E. B. Fernandez, "Threat modeling in cyber-physical systems," in *Proc. nd Intl Conf Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech) 2016 IEEE 14th Intl Conf Dependable, Autonomic and Secure Computing, 14th Intl Conf Pervasive Intelligence and Computing*, Aug. 2016, pp. 448–453.

[20] M. Rekik, C. Gransart, and M. Berbineau, "Cyber-physical threats and vulnerabilities analysis for train control and monitoring systems," in *Proc. Computers and Communications (ISNCC) 2018 Int. Symp. Networks*, Jun. 2018, pp. 1–6.

[21] Y. Atif, Y. Jiang, D. Jianguo, M. Jeusfeld, B. Lindström, S. Andler, C. Brax, D. Haglund, and B. Lindström, "Cyber-threat analysis for cyber-physical systems," 2018.