Identifying the best Methods for Passive and Active Cybersecurity Assessment

Iwan Grinwis
University of Twente

ABSTRACT

Companies currently struggle with the right way to assess their cybersecurity, due to the fast-growing industry and a large number of methods available to assess it. NIST proposed 5 functions every company should comply with in order to reduce cyber risks, but once again there is close to no literature available on what methods to do this will best protect the company. In this paper, we intended to find out what set of methods for both passive and active cybersecurity would provide a company with the most complete cybersecurity assessment while taking the NIST proposed functions into consideration. To achieve this, we analyzed a set of methods, compared them in tables to each other, and pointed out the advantages and shortcomings of the methods. We proposed 4 sets of methods that cover the most NIST functions and provides the company with the most complete experience, covering a lot of aspects.

1. INTRODUCTION

Currently, cybersecurity assessment can be performed using a lot of different methods. Although a lot of third-party companies offer cybersecurity assessment, it is unclear what methods are considered the best or most well fit for a company. To tackle this, the National Institute of Standards and Technology (NIST)[9] came up with 5 functions that every company should comply with to properly protect themselves against cyber risks. The 5 functions are identify, protect, detect and respond against threats[20]. But once again, there is minimal information available over what methods can comply with these 5 functions.

Threats are potential attacks on assets (e.g., information /data, applications/information systems/ software, devices, and stakeholders) and consequently on business processes. There are thousands of attacks exploiting vulnerabilities on different assets and every single one of those attacks can bring several risks with it. Each risk can be classified in a few aspects, such as the severity level and the likelihood. Towards assessing the security of a company all of these aspects should be considered.

There are two ways to assess the security of a company: passive[2] and active[2] cybersecurity assessment. Both assessment methods intend to sketch out the cybersecurity risks the company currently has and what the characteristics (for example the severity level) of these risks are.

Passive assessment[26] involves using threat model methods, which intend to look at more passive related security topics for a company. The passive side of it implies that it does not interact with the system, in contradiction to active cybersecurity assessment. A good example of this is a minimum amount of characters on an employee password – to reduce the threat of a brute force attack.

Active assessment is about the risk and vulnerability assessment, which intention is to look at activity-related risks. This means that the tools or methods to do this interact with the system, for example they can try and penetrate it. This involves the security risks around who can open a certain file and how assets are being accessed by employees or hackers.[16]

The goal of this paper is to survey passive and active security assessments towards identifying the best methods for a comprehensive qualitative assessment. To pursue our goal, we have defined the following research questions (RQ) as the basis of our research.

- **RQ1:** What are the characteristics of security threat models?
- **RQ2:** What are the characteristics of risk and vulnerability assessment?
- **RQ3:** What set of threat models and risk and vulnerability assessment provides the most complete security assessment of a company?

In this paper, we researched the most used passive and active cybersecurity assessment methods to find out which set of those methods would cover the most security activities, while also explaining why this set would be better than other sets of methods. We will focus our research on the first three activities proposed by NIST: Identify, protect and detect, since these three activities can be covered by assessment tools, the other two require guidelines on how to act after an attack, while assessment tools are meant to prevent an attack from happening in the first place.

The remainder of this paper is organized as follows. Section 2 will discuss the related works, the five NIST functions and provide some explanation about how certain active and passive assessment tools work, section 3 will contain our methodology and approach, and section 4 will contain the results. At the end of the paper, there will be a conclusion in which we summarize the work we have done, the results, state the limitations of our work and provide a recommendation for future works.

28^{th} *Twente Student Conference on IT* Febr. 2^{nd}, 2018, Enschede, The Netherlands.

2. RELATED WORK AND BACKGROUND INFORMATION

In this section, we will show some related works to our research. We will also explain some basic background information, which is necessary to understand the results of our research.

2.1 Related works

The works we look for are works that compare or analyze the available methods for passive and active cybersecurity assessment. In "A comparison of cybersecurity risk analysis tools"[24] the authors do a comparison showing the differences between a few available cybersecurity risk management tools. However, one of the less relevant parts of this research is that it goes into great depth about tools being used for active cybersecurity, while we want to look at the methods behind those tools.

A really recent work on the same topic is "Review of Cybersecurity Assessment Methods: Applicability Perspective[14]. In this work the author points out that currently there are very few available reviews cybersecurity assessment methods, which is the same problem as we pointed out. One of the key differences of this research is that it mostly discusses the actual tools. For example, it compares a lot of different penetration testing tools with each other, while we are mostly interested in the actual method of penetration testing as a whole.

2.2 NIST five function model

In the introduction we spoke about the five functions NIST proposes that every company should do in order to protect themselves from cyberattacks. We will introduce the five functions here.

The identify activity of the NIST cybersecurity framework is the first activity a company should take and is logic wise the first step of the full activity circle. To comply with this function, companies must develop and understand their environment to manage the cybersecurity risks to systems, data and assets. Examples of activities are: full visibility of digital and physical assets and their interconnections and making sure the company knows their risks and exposures and put policies or procedures in place to manage or reduce those risks. This step is necessary to take before a company can proceed with step two, as you can't protect yourself if you don't know what you are protecting.

The protect activity requires a company to outline appropriate safeguards to ensure the critical infrastructure of the company to keep working. The protect activity is established that in case of a cyberattack, the impact will be as limited as possible. Examples of activities that can take place in this function are employee awareness training (to prevent phishing attacks) or protocols for user access (requirements to a password, ways of identification for an employee)

The detect activity is focused on allowing the company to quickly react in case of a cyber attack. This means that in case a malicious event occurs, the company should have policies in place that make sure this event is detected timely to reduce the impact of the attack. Examples of activities that take place here are the creation or placement of a network intrusion detection system and making sure that the company always has insights in their current networks.

The other two functions defined by NIST are respond and recover, which are not relevant to our research. Therefore we will not go in-depth about those two.

2.3 Passive and active cybersecurity assessment methods

We will shortly introduce the passive cybersecurity assessment methods, this can be used as a glossary to later come back to in case knowledge about the method is assumed.

- The Common Vulnerability Scoring System (CVSS) is a system that scores threats based on how severe these are. It works with a weighted calculator.[22]
- STRIDE is a threat model methodology that looks at a system and asks the question: "What could go wrong?". It includes a full breakdown of the system's processes, data stores, data flows & trust boundaries.[8]
- PASTA is a framework that consists of 7 stages, which includes way more than just a threat model. (It includes things like Risk & Impact analysis & defining business objectives)[7]
- LINDDUN is a 3 step framework with the following steps: Model the system, Elicit threats and Manage threats.[5]
- Attack Trees are a technical way of modeling security threats. It is mostly used as a part of other threat models. It includes a step-wise diagram of how a certain part of a system is accessed. (to find out where it can go wrong)[25]
- Persona Non Grata (PnG) has its focus on the person behind an attack instead of the threat itself. It considers motivations and skills needed, forcing analysts to look at the system from the attack point of view.[19]
- Security Cards is a method that uses a deck of cards to answer questions like: "who might attack? and "why will they attack?". It is more of a brainstorming technique rather than a formal method. [19]
- Trike is a risk model which includes a threat model in its method. It is based on assets, roles, human actions, and calculated risks. [6]
- Visual, Agile, and Simple Threat (VAST) is a threat model that makes two types of models: Application threat models & operational threat models. This allows you to view both the architectural and the attacker's point of view.[31]

The following 7 active cybersecurity assessment methods will be discussed and considered in the paper.

- Network mapping is a method to visualize your network and every device connected to it. The point of it is to generate easy to understand graphical images on how the devices on your network are performing.[10]
- Vulnerability scanning is an inspection of potential entry/exploit points on a computer or a network. Normally you would attempt 2 different scans: authenticated and unauthenticated. Authenticated means finding out what an employee can access/exploit, while unauthenticated is what anyone can do.[1]
- Phishing assessment is an inspection of employee awareness in a company. The method is focused on contacting employees with phishing attempts and find out how they respond to it.[4]

- Web-app assessment is a vulnerability scan specifically for web applications. The goal is to find all vulnerabilities and provide the company with ways to patch those.[3]

- OS security assessment is a vulnerability scan specifically targeted at the firewall, antivirus, intrusion detection software, and any other type of cybersecurity software that is running on the system.[23]

- Database assessment is a vulnerability scan targeted at databases, using known vulnerabilities and different attack scenarios.[11]

- Penetration testing is a simulation of a cyber attack against a company, meaning it will try anything to get into the system.[12]

3. METHODOLOGIES

In this section, we will go into detail about the steps we took to answer our research questions. The first step in our progress was defining the research questions, as creating those would highlight the scope of our research. RQ1 and RQ2 are used to gather all the information required to answer RQ3.

Once we knew the scope of our research, we had to look for relevant works/papers. We used the following keywords: 'Cybersecurity Risk Assessment' and 'Cybersecurity Threat Assessment'. For both keywords, we selected the top 5 results and the top 5 most quoted papers (which in some cases were mostly the same papers). We aimed for papers that were written or published after 2017 since we want to look at the current state of those assessment tools as the industry is a very fast-growing and evolving industry. After selecting those papers, we would look at their relevance.If we considered a paper to be relevant, we would look at works related to this paper as well and once again take a look if they would be relevant for us.

After finding relevant papers, the next step was to find the characteristics for both passive and active cybersecurity assessment methods. We used the available literature to find the characteristics and note them down in a table. (Literature can be found in the background information section) This table makes our work for RQ3 a lot easier since we will be able to easily see what the advantages and disadvantages of a certain method are.

But before we could work on RQ3, we first had to identify and define the five security activities proposed by NIST (Mostly the first three) in a more detailed way. We had to find out what was required to fulfill a certain activity, so we could later find out which methods would cover what activity. After researching all of this, we made some conclusions and came up with some/a proposed set of methods which based on our research would be the best set of methods for those security activities.

4. RESULTS

In this section, we will discuss the findings for every research question. We will start by explaining the characteristics of threat models, followed by risk & vulnerability models. Then we will compare the methods to the NIST functions. Finally, we will answer the question of which set of those methods is the best taking the principles of NIST into consideration.

4.1 Threat models (RQ1)

We first have to define what a threat model method is. "a threat modeling method (TMM) is an approach for creating an abstraction of a software system, aimed at identifying attackers' abilities and goals, and using that abstraction to generate and catalog possible threats that the system must mitigate."[27] In other words, the general rule for a threat model would be: A threat model method is a way of identifying threats.

The way a threat model does what its definition stated, is different for every threat model method. Some take a look at the threat itself (CVSS, Attack Trees), while others take a look at the full system from an attacker's point of view (PASTA, PnG). For our research, we will limit ourselves to the threat models named in the background information section of this paper. We will also talk about some other models which consist out of combinations of the earlier mentioned models.

Since the first part of our research consists out of finding the characteristics of cybersecurity threat models, we started off with creating a table that includes the threat model methods and some of the main characteristics.

In Table 1 we show the main characteristics of threat model methods. We split the table into 4 different sections: the perspective, the pros, the cons, and the other notable characteristics. The perspective indicates the way of approach; an attacker view indicates that the method starts from the attacker's point of view and looks at the system to find threats while a system view starts by mapping the system and then attempts to find threats. The pro's that are mentioned are some of the advantages of using this method in comparison to other methods, meaning we intended to not have too many duplicates in this section (example: If a lot of methods can be done by the company instead of a third party, then it would not be a pro since a lot of them would just have the same pro, making them not stand out). The same holds for cons, which names some of the disadvantages of the method. Other notable characteristics are used to better describe the method, or mention a unique characteristic of the method.

When we analyze all methods, we notice that CVSS is the only method that lacks a perspective. The reason for this is that CVSS does not detect threats itself, it is only used as an indication of the severity of the threat.

Another important fact is that a few methods can not work on their own. CVSS, LINDDUN, Attack Trees, PnG, and Security Cards are all considered to be not broad enough to work on their own. The reasons can be read in the cons part of the table. For these methods hold that most of them are used in combination with other methods, for example in threat model methods like Hybrid Threat Modeling Method (hTMM)[18], which is a made using a combination of PnG, Security Cards, and STRIDE.

The only two threat model methods that rely solely on a system breakdown/system perspective are LINDDUN and Trike. LINDDUN is more of a method that helps in the design phase and is used as a checklist of which privacy and security practices should be present in a system. Trike is used for risk management within assets and approaches the system by stating for every asset the allowed level of risk. Since both Trike and LINDDUN are considered as different from the other threat model methods in terms of goal (risk and privacy), we can state that both of them fall out of the standard trend of a threat model method.

Threat model characteristics				
Threat model method	**Perspective**	**Pro's**	**Cons**	**Other notable characteristics**
CVSS	N/A	Gives an indication what threats are more important/severe then others	Cannot perform on its own due to the lack of a threat detection method	Commonly used together with other threat model methods
STRIDE	Attacker view	Can be used as a checkbox for other methods afterwards, making sure that they did not miss a category.	Really old, other more recent methods cover more relevant threats	Full system coverage
PASTA	Attacker view	Direct contribution to risk management and is also a very extensive method	Since it incorporates business impact analysis, many more people are involved, who all might need training[21]	Really time consuming, making it a really hard to execute method
Attack Trees	Attacker view	The method gives a very systematic overview of a threat, making it easy to see where the security issue lies	Since it only focuses on single threats, it on it self is not broad enough to be used solely	Usable on single threats
PnG	Attacker view	It focuses on humans instead of focusing on a system, granting a unique point of view on threat modelling	Won't function on itself as it solely shows what systems might be exposed, not what threats are present in it	The goal is to create profiles of possible hackers, which is a very unique way of thinking
Security Cards	Attacker view	Mostly used together with other methods to provide the team with some unique insights	Does not function on its own simply because it is to simplistic and not in depth enough	Brainstorming technique
Trike	System view	Unique way of creating a threat model, uses a risk requirement to say for each asset what the allowed level of risk is.	Can be really hard to execute on large scale systems since you will have to map the entire system	Way more then just a threat model, covers a lot of risk related problems as well
LINDDUN	System view	Focuses heavily on privacy threats	Since it mostly focuses on privacy threats, it on it self can be considered as not broad enough to be to be used solely	Can be very time consuming the bigger the system gets
VAST	System & Attacker view	Very scalable, making it a very useful method for large companies	Doesn't have a very good publicly available documentation	Direct contribution to risk management

Table 1. Characteristics of cybersecurity threat models.

Risk and vulnerability models			
Method name	**Scope**	**Pro's**	**Cons**
Network mapping	Network properties	Automated tools are available, reducing the time and effort	Does not directly show any risks or vulnerabilities
Vulnerability scanning	Entire system	automated tools are available, reducing the time and effort	Does the same as a penetration test, except a penetration test just does it better
Phishing assessment	Employees	Covers the human vulnerability of a company	Can be a risk to employee privacy
Web application assessment	Web applications	automated tools are available, reducing the time and effort	Does the same as a penetration test, except a penetration test just does it better
Operating system security assessment	OS	Helps in the detection part of a system, since it assesses the intrusion detection systems and firewalls	Not a lot of information about how to perform this task is available
Database assessment	Database	Covers one of the most important parts of a company that can be at great risk if hacked	N/A
Penetration testing	Entire system	Covers a lot of other risk and vulnerability models as well	Can be really expensive and time consuming, as it almost always require a third party to perform this task

Table 2. Risk and vulnerability models.

4.2 Risk and vulnerability models (RQ2)

As stated before, a threat modeling method is an approach to create an abstraction of a software system, which is used to catalog possible threats in the system. In other words, a threat is what a company is defending itself against. A vulnerability is a weakness that undermines the companies IT security efforts, for example, a flaw in a system that allows a hacker into their database. Risk is a combination of the two;

$$risk = threat\ probability * vulnerability\ impact$$

.[15] This means that when looking at the risk it will put the probability of a threat against the impact of this potential vulnerability.

In Table 2 we can view the selected risk and vulnerability model methods, and four attributes connected to every method. The four attributes are 'target', 'pro's and cons'. In the target attribute, we state what the target of the method is, so what part of a company or system does it cover? The pros are the advantages of a method, while the cons are the disadvantages of a method.

After looking at the table, we can draw the conclusion that a penetration test offers by far the most complete and in-depth experience. Both vulnerability scanning and web application assessment are almost completely covered by it, and for both of them, penetration testing even goes a step further by not only finding the exploit but also attempting to exploit it and see what information is being yielded from it.

Another very important risk and vulnerability model method which we can conclude from Table 2 is phishing assessment. Phishing assessment is the only method that considers the human factor in a company. As a company, you can protect yourself as much as possible, but if your employees are not aware of phishing attacks and fall for them, it can still have a huge impact on your company. The downside of phishing assessment is that it can be a risk to the privacy of your employees since name shaming can be a really bad thing. This can be solved by using redirect links which can count the number of times it is clicked instead of finding out who clicked it.[29] However, the downside of this approach is that it requires you to train the entire company instead of just training the employees that fell for it, which can be very time-consuming and costly.

4.3 What set of threat models and risk & vulnerability assessment provides the most complete security assessment of a company? (RQ3)

Before we can answer the question of what set of methods provides the most complete experience, we first have to see what part of the NIST five functions[20] are being covered by every methods we discussed in 4.1 and 4.2. More explanation about the five functions of NIST can be found in the background information section of this paper.

Table 3 contains the methods and the three discussed functions, we won't be covering respond & recover since cybersecurity assessment methods are methods to prevent cybersecurity attacks from happening in the first place, while respond and recover are functions that come after an attack has happened.

The column A/P explains whether the method is an active or a passive cybersecurity assessment method. To provide some clarification: The A/P category means Active/Passive. An x indicates that the method does cover the activity and a - means the method does not cover it. When we say that a method covers it, we say that the method contributes to covering this activity, which may vary for different methods.

After analyzing Table 3 we notice that the only methods that cover detect are the OS security assessment tool and penetration testing. The reason these two activities cover it is due to the fact that both of them assess systems that are made to do the detect functionality themselves. The OS security assessment assesses the firewalls and intrusion detection systems, which means that doing this assessment actually helps in improving the detection activity of the company. The same holds for penetration testing since penetration testing tries to get into the system in every possible way, meaning it will also attempt to bypass a firewall or not trigger an intrusion detection system, meaning it will help in improving this system.

Furthermore, we notice that CVSS is the only method that does not cover the identify function. Since CVSS is merely used for the severity scoring of a threat, it does not contribute anything in regards to the identification of cybersecurity threats to a company.

The last observation we make in regards to Table 3 is the fact that Security Cards does not cover the protect function. Security Cards is a method that is more of a brainstorming technique rather than a threat model since it consists out of a pile of cards containing questions about possible motives/attacks. Because of this, it does not contribute to the protect function as it does not cover any questions in regards to the system itself.

Now that we know what the 5 functions of NIST are, we will define the other terms used in the question. What is the goal of a threat model, what is the goal of risk and vulnerability assessment models, and what is the definition of a complete security assessment?

The goal of a threat model is to answer the question: What threats, taking the ability and goals of the attacker into consideration, should our system be able to mitigate? We can come up with the following requirements:

- Requirement 1: It should be able to identify threats
- Requirement 2: It should be able to take the abilities and goals of an attacker into consideration
- Requirement 3: It should provide some way of analyzing whether or not it is an acceptable threat/risk

The goal of a risk and vulnerability assessment model is to answer the question: What are the actual vulnerabilities of my system and what are the risks and impacts of someone exploiting them? We can come up with the following requirements:

- Requirement 1: It should be able to identify independent vulnerabilities
- Requirement 2: It should be able to find out the risks of someone exploiting them

Finally, the definition of a complete security assessment of a company can be derived from the NIST 5 function principle. We can come up with the following requirements to cover the first 3 (identify, protect and detect) cybersecurity functions proposed by NIST:

- Requirement 1: The set of methods should be able to identify possible risks to systems, data, and assets in their environment to the best extend

NIST 5 activity principle combined with cybersecurity assessment tools				
method name	**A/P**	**Identify**	**Protect**	**Detect**
CVSS	P	-	x	-
STRIDE	P	x	x	-
PASTA	P	x	x	-
LINDDUN	P	x	x	-
Attack Trees	P	x	x	-
PnG	P	x	x	-
Security Cards	P	x	-	-
Trike	P	x	x	-
VAST	P	x	x	-
Network mapping	A	x	x	-
Vulnerability scanning	A	x	x	-
Phishing assessment	A	x	x	-
Web-app assessment	A	x	x	-
OS security assessment	A	x	x	x
Database assessment	A	x	x	-
Penetration testing	A	x	x	x

Table 3. Cybersecurity assessment tools.

Proposed sets of methods					
Sets	**Passive security**	**Passive security**	**Passive security**	**Active security**	**Active security**
Large company big budget	VAST	CVSS	PnG	Phishing Assessment	Penetration Testing
Small company big budget	hTMM	CVSS	-	Phishing Assessment	Penetration Testing
Small company small budget	hTMM	CVSS	-	Phishing Assessment	Vulnerability scanning
Large company small budget	VAST	CVSS	PnG	Phishing Assessment	Vulnerability scanning

Table 4. Proposed set of methods complying with the requirements

- Requirement 2: The set of methods should be able to help with protecting the company against cyber risks to the best extend
- Requirement 3: The set of methods should be able to help in detecting possible cyberattacks, by testing and analyzing the systems in place to this job

Now that we know the requirements and explained the question we intend to answer, we will start by explaining a method that has not yet been discussed here or compared with other methods. The Hybrid Threat Modeling Method (hTMM)[17] [13] is a method that consists out of elements of three other threat model methods: STRIDE, PnG, and Security Cards. It uses the checklist that STRIDE provides, models the potential attackers using PnG, and finally questions the potential risks of these attackers by asking the questions that Security Cards bring to the table.

We can state that hTMM can be considered as one of the methods for a set of methods that we will propose since it does cover 2 out of 3 requirements of our ideal threat model, as can be derived from Table 3 by looking at Security Cards, STRIDE and PnG. By adding CVSS we can get an even better indication of how severe a threat is, which would add a lot of value to the final set as well. The downside of this set of methods would be that hTMM is not a very scalable method, meaning the bigger the system gets, the more complex and time-consuming this method will be. The final verdict for this set of threat model methods would be that it could be the best for small companies but will fall off once companies become bigger and bigger.

Another set of threat models we can consider would be VAST combined with CVSS and PnG. VAST is considered one of the best[30] threat models due to its very good scalability, due to using automated tools instead of manual threat modeling. Together with PnG (To cover the human factor) and CVSS (to indicate the risks of individual threats), it covers all 3 requirements.

Now that we found two sets of methods for passive cybersecurity, we move on to active cybersecurity. Finding the right methods for active cybersecurity proves to a bit more difficult, as most of the methods we selected have completely different goals; some focus purely on the database while others cover the human aspect of cybersecurity. Judging from our requirements, most individual methods would fulfill the requirements, but only partly. If a company does a database assessment, it fulfills both requirements 1 and 2, but only for the database.

Because of this, we will have to look at what parts of the system prove to be the most important and most attacked parts. According to Varonis (which is a big security company located in the US) 88% of all organizations worldwide were targeted by phishing attacks in 2019[28]. According to Verizon[32], 45% of the breaches that occurred were caused by hacking, 22% involved phishing, and 17% involved malware[28]. What this means to us, is that especially phishing and hacking are the two main cyberattacks. To counter phishing, we can use phishing assessment as an active cybersecurity method. For hacking, both vulnerability scans and a penetration test would do the trick, however, a penetration test is more of a simulation whereas a vulnerability scan only scans for known vulnerabilities. As stated in table 2, a penetration test is mostly just a vulnerability scan that goes a step further by simulating an attack. The downsides for phishing assessment, as named in table 2, are not that big so can be neglected. For penetration testing, it is a different story, as penetration testing can be a very expensive assessment method. The cheaper alternative that should yield relatively the same results (be it slightly worse) is the vulnerability scan.

These sets of methods can be viewed in Table 4. These methods will provide a company with the most complete experience in regards to their cybersecurity, while also complying with all 3 of the discussed functions proposed by NIST.

5. CONCLUSIONS

In this paper, we selected a list of both active (risk & vulnerability assessment) and passive (threat assessment) methods in order to find out what set of these methods would be the best fit for a company in regards to the 5 functions proposed by NIST. We analyzed every method by figuring out how it worked, what kind of results it would yield, and what literature is available about the method. We then compared the methods with each other and came up with four sets of methods for different scenarios. We took into consideration the budget a company is willing to spend on it and how big of a company it is. The sets can be viewed in Table 4.

In conclusion, we can state that hTMM combined with CVSS, phishing assessment, and penetration testing will provide a small company with a big budget the best result. However, due to every company being different, we also look at other scenarios. Vulnerability scanning is the cheaper alternative for companies, providing relatively the same results as a penetration test but doesn't do the last step of penetration testing, which is exploiting the vulnerability.

VAST and hTMM also yield relatively the same results, however, VAST is an automated threat modeling method and scales better when a company grows. For this reason, if a company is considered big, we would advise using VAST instead of hTMM.

Some limitations to our research are present since we do not have any user experience with any of these methods. The results are based on the available literature on each of these methods and our critical analysis of this literature. To extend this research, a good approach would be to test the sets of methods proposed in practice.

References

[1] Balbix. What to know about vulnerability scanners and scanning tools balbix. https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/, 07 2020. (Access on 17/6/2021).

[2] S. Brathwaite. Active vs passive cybersecurity reconnaissance in information security securitymadesimple. https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security, 01 2021. (Access on 27/6/2021).

[3] Centric. How secure is your web application. https://www.centric.eu/en/solutions/cyber-security-services/web-application-assessment/, 08 2020. (Access on 17/6/2021).

[4] Compass. Phishing assessments compass it compliance. https://www.compassitc.com/services/phishing, 08 2020. (Access on 17/6/2021).

[5] DistriNet. Linddun linddun. https://www.linddun.org/linddun, 09 2020. (Access on 17/6/2021).

[6] EC-Council. Trike threat modeling as a riskmanagement tool eccouncil official blog. https://blog.eccouncil.org/trike-threat-modeling-as-a-risk-management-tool/, 12 2020. (Access on 17/6/2021).

[7] EC-Council. What is pasta threat modeling eccouncil official blog. https://blog.eccouncil.org/what-is-pasta-threat-modeling/, 12 2020. (Access on 17/6/2021).

[8] EC-Council. What is stride methodology in threat modeling. https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/, 10 2020. (Access on 17/6/2021).

[9] U. S. government. National institute of standards and technology nist. https://www.nist.gov/, 02 1997. (Access on 25/6/2021).

[10] D. Hein. What is network mapping and how does it help network performance. https://solutionsreview.com/network-monitoring/what-is-network-mapping-and-how-does-it-help-network-performance/, 01 2019. (Access on 17/6/2021).

[11] Imperva. Database security assessment. https://www-356.ibm.com/partnerworld/gsd/showimage.do?id=24046, 2007. (Access on 17/6/2021).

[12] Imperva. What is penetration testing step-bystep process methods imperva. https://www.imperva.com/learn/application-security/penetration-testing/, 04 2019. (Access on 17/6/2021).

[13] S. Krishnan. A hybrid approach to threat modelling a hybrid approach to threat modelling. https://www.researchgate.net/publication/320183133_A_Hybrid_Approach_to_Threat_Modelling_A_Hybrid_ 02 2017.

[14] R. Leszczyna. Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, page 102376, 2021. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2021.102376. URL https://www.sciencedirect.com/science/article/pii/S0167404821002005.

[15] Lifars. Threat vulnerability risk what is the difference. https://lifars.com/2020/07/threat-vulnerability-risk-what-is-the-difference/, 07 2020. (Access on 8/6/2021).

[16] Marie-Pier. Do active and passive risks have the same predictive power as cybersecurity behaviour konnect. https://konnect.serene-risc.ca/2020/10/22/do-active-and-passive-risks-have-the-same-predictive-power-as-cybersecurity-behaviour/, 11 2020. (Access on 27/6/2021).

[17] N. Mead and F. Shull. The hybrid threat modeling method. "Carnegie Mellon University's Software Engineering Institute Blog", 2018. URL "http://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/".

[18] N. MEAD and F. SHULL. The hybrid threat modeling method. https://insights.sei.cmu.edu/blog/the-hybrid-threat-modeling-method/, 05 2021. (Access on 18/6/2021).

[19] N. Mead, F. Shull, K. Vemuru, and O. Villadsen. A hybrid threat modeling method. Technical Report CMU/SEI-2018-TN-002, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2018. URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617.

[20] U. G. NIST. The five functions nist. https://www.nist.gov/cyberframework/online-learning/five-functions, 01 2019. (Access on 8/6/2021).

[21] L. Nweke and S. Wolthusen. A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications*, 11: 1–6, 03 2020. doi: 10.14569/IJACSA.2020.0110201.

[22] F. of Incident Response and S. Teams. Cvss calculator. *https://www.first.org/cvss/calculator/3.0*, 2021.

[23] U. of Maryland. Operating system security assessment reporteditteddocx running head operating system security assessment report operating system security assessment course hero. https://www.coursehero.com/file/39636033/Operating-System-Security-Assessment-Reporteditteddocx/, 01 2019. (Access on 17/6/2021).

[24] G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadão, I. Yevseyeva, and V. Basto-Fernandes. A comparison of cybersecurity risk analysis tools. *Procedia Computer Science*, 121: 568–575, 2017. ISSN 1877-0509. doi: https://doi.org/10.1016/j.procs.2017.11.075. URL https://www.sciencedirect.com/science/article/pii/S1877050917322755.

[25] B. Schneier. Academic attack trees schneier on security. https://www.schneier.com/academic/archives/1999/12/attack_trees.html, 05 2016. (Access on 17/6/2021).

[26] N. Shevchenko. Threat modeling 12 available methods. https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/, 04 2021. (Access on 20/5/2021).

[27] F. Shull. Evaluation of threat modeling methodologies. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=474197, 2016. Accessed: 20/05/2021.

[28] R. Sobers. 134 cybersecurity statistics and trends for 2021 varonis. https://www.varonis.com/blog/cybersecurity-statistics/, 11 2018. (Access on 18/6/2021).

[29] L. Spitzner. Phishing assessments a simple anonymous and free approach. https://www.sans.org/blog/phishing-assessments-simple-anonymous-and-free-approach/, 10 2012. (Access on 18/6/2021).

[30] Threatmodeler. Threat modeling methodologies what is vast threatmodeler. https://threatmodeler.com/threat-modeling-methodologies-vast/, 10 2018. (Access on 18/6/2021).

[31] threatmodeler. Security threat modeling methodologies comparing stride vast more. https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business/, 06 2020. (Access on 17/6/2021).

[32] Verizon. Enterprise technology solutions verizon. https://www.verizon.com/, 01 2021. (Access on 18/6/2021).