Tampere University

Sini Kivioja

INFORMATION SECURITY THREAT AND RISK ASSESSMENTS IN DEVOPS

Bachelor’s thesis
Faculty of Information Technology and Communication Sciences
October 2022

ABSTRACT

Sini Kivioja: Information Security Threat and Risk Assessments in DevOps
Bachelor's thesis
Tampere University
Information Technology
October 2022

Information Security (IS) is becoming increasingly important in a modern digitalized world. Almost anything can be done online, which has become an opportunity for cyber incidents.

Risk analysis and threat modeling are ways to find and mitigate risks and threats in organizations and its assets. DevOps is also becoming increasingly popular in software development. The idea of DevOps is to make the software development process faster and more efficient. One of DevOps' practices is security, yet there have still been problems with incorporating security into DevOps.

This thesis studies different kinds of threat modeling and risk analysis methods. The methods are presented and then analyzed according to their features. The methods are ISO 27005, CORAS, OCTAVE, FAIR, STRIDE and CTM.

The results of this study show that there is no absolute answer on which one is the best for DevOps processes. There were good factors in all the methods, but they also all had room for improvement. Therefore, the thesis cannot claim that there would be one perfect assessment method in the studied methods. ISO 27005 is considered as a good overall method for risk analysis, although there needs to be more studies on its compatibility for DevOps. STRIDE was often used with DevOps, but it has its downsides. The "shift left" and especially continuity have been noticed to be a good factor in threat and risk assessment methods. Continuous Threat Modeling is a new unstudied analysis method, that has a very promising idea when thinking about DevOps.

Security in DevOps and especially risk analysis and threat modeling are subjects that should be researched more in the future.

Keywords: DevOps, DevSecOps, risk analysis, threat modeling, assessment, information security

TIIVISTELMÄ

Sini Kivioja: Riskianalyysit ja uhkamallintaminen DevOpsissa
Kandidaatintyö
Tampereen yliopisto
Tietotekniikka
Lokakuu 2022

Tietoturvallisuudesta on tullut todella tärkeä asia digitalisoituvassa maailmassa. Melkein mitä tahansa pystytään tehdä internetissä, mikä on luonut mahdollisuuden kyberonnettumuuksille. Riskianalyysit sekä uhkamallintaminen ovat tapoja eliminoida riskejä ja uhkia organisaatioissa ja suojella organisaation omaisuutta. DevOps on myös kasvattanut suosiotaan ohjelmistokehityksessä. Sen ideana on tiivistettynä tuottaa nopeasti ja tehokkaasti uutta koodia ohjelmistokehityksessä.

Vaikka DevOpsin yksi ominaisuuksista on tietoturva, on sen sisällyttämisessä ilmennyt ongelmia. Tässä kandidaatintyössä käydään läpi erilaisia uhkamallinnus- sekä riskianalyysitapoja, ja niiden soveltuvuutta DevOpsiin. Aluksi käsitellään kirjallisuuskatsaukseen liittyvää teoriaa, jonka jälkeen siirrytään analyysitekniikoihin ja niiden ominaisuuksiin. Tutkielmassa esitellään kuusi erilaista riskianalyysi- tai uhkamallinnusmetodia. Nämä metodit ovat ISO 27005, CORAS, OCTAVE, FAIR, STRIDE sekä CTM. Metodit on valittu niiden hyvän dokumentoinnin takia, ja lisäksi tulevaisuutta ajatellen on mukaan otettu uudempi, vähemmän tutkittu CTM-metodi.

Opinnäytteen tutkimusten mukaan ei ole yhtä oikeaa tapaa tehdä riskianalyysejä. Analyysien jatkuvuuden on huomattu olevan yksi tärkeä tekijä DevOps-ympäristöissä. Lisäksi esimerkiksi yhteisöllisyyden, nopeuden ja turvallisuuden on sanottu olevan tärkeitä DevOpsissa. Continuous Threat Modeling:n idea vastaa jatkuvuuskysymykseen, vaikka onkin uusi ja huonosti tutkittu metodi. ISO 27005 todettiin hyväksi yleisanalyysimetodiksi. STRIDE:ä on usein käytetty DevOpsin kanssa. Kaikista työssä tutkituista metodeista löytyi jotakin hyvää ja jotakin parannettavaa, joten ei voida varmasti sanoa absoluuttista parasta metodia DevOpsiin.

DevOpsiin liittyvään tietoturvaan, etenkin uhkamallintamiseen ja riskianalyyseihin, tulisi tehdä lisää tutkimusta tarkempien tuloksien saamiseksi.

Avainsanat: DevOps, DevSecOps, riskianalyysi, uhkamallinnus, tietoturva, kyberturva

CONTENTS

1. INTRODUCTION

Information security has become a crucial part of organizations, especially in software development. In recent years, cyber-attacks, privacy information loss and a lot of unwanted incidents have been witnessed. Some of these could have been mitigated with the right security practices.

In this thesis, the focus is on one of the most important parts of DevOps: security, and threat and risk assessments in particular. These assessments are important in order to mitigate risks and to avoid harmful incidents.

The thesis is made to study the possible ways of performing the threat and risk assessment for DevOps. There are a few different types of risk assessment and threat modeling techniques covered. There are some differences and similarities between risk analysis methods and threat modeling. Initially, both methods try to find risks and threats so that the organization can eliminate or mitigate these. The reason these methods are chosen for this thesis is that they are well documented and often used in IT organizations. There is also a newer CTM method that is less studied but has some potential factors when thinking of DevOps.

The thesis is structured as follows. Chapter 2 defines the theoretical background of this thesis. It introduces the concepts of information security, assets, risk, DevOps and DevSecOps, that give the base of this thesis. In chapter 3 the theory is expanded to the threat and risk assessment methods and their qualities. ISO 270005, CORAS, CIRA, FAIR, STRIDE and CTM are presented in this chapter. STRIDE and CTM are considered as "threat modeling", and others "risk analysis". The results of this thesis are presented in chapter 4. Chapter 5 gives a conclusion of the findings in this thesis and gives an idea of what could be done in the future in this field.

2. THEORY

Information security has become important in the recent years. To fully understand threat modeling and risk analysis, we must understand some key parts of information security.

Information security measures try to protect the following aspects: confidentiality, integrity, and availability of information. These security goals form the CIA triad. Confidentiality stands for information not being made available to unauthorized processes, entities, or individuals. Integrity means those security controls needed to detect data modification or substitution because of unauthorized access. Availability in this context is the capability to access the information when chosen. In addition, information security can try to preserve the authenticity, accountability, non-repudiation, and reliability of the information. (ISO Central Secretary, 2020)

ISO (International Organization for Standardization) 27000 states that organizations need to monitor the success of used controls and procedures. They should also identify risks that need to be treated and implement the right security controls. When security controls are implemented, they are expected to work seamlessly with the organization's business processes. (ISO Central Secretary, 2020)

2.1 Asset

An asset is usually described as "anything that has value to the organization", and because of that, it needs protection (ISO Central Secretary, 2020). Assets can be classified as physical, logical, or human assets. Physical assets are any physical components that an organization has. Logical assets contain information - they can be algorithms, knowledge, or proprietary practices. Human assets include people, their skills and knowledge. (ISO Central Secretary, 2013)

It can be difficult for the organization to have a secure environment if they don't understand what they are protecting.

2.2 Risk

To understand risk, threat and vulnerability needs to be determined first. A threat is an unwanted incident that may outcome in damage, loss or disclosure to an organization or system (ISO Central Secretary, 2020). Threat could be for instance error, malicious code, fraud, or theft.

Vulnerabilities are weaknesses that are part of systems, organizations or components (ISO Central Secretary, 2013). Vulnerabilities can allow a threat agent to gain unauthorized access to organizational assets (ISO Central Secretary, 2020). If there were no vulnerabilities, there wouldn't be any risks either.

ISO Central Secretary, 2020 states in ISO 27000 that risk is the "effect of uncertainty of objectives". It is related to the possibility that threats will exploit vulnerabilities of assets and can cause damage to organizations. Risk can also be defined by probability times damage potential (Microsoft, 2010). By one definition, the net risk can be equal to inherited risk where the controls in action are reduced (Georgeta and Alexandru, 2017). The outcome of risk can be e.g., loss of privacy data or loss of money.

In this thesis, we think of risk as a combination of these definitions.

2.3 DevOps

DevOps can be defined in many ways, but the main idea is to shift the software development process "to the left". "DevOps" comes from a combination of the words "development" and "operation". This means that development and operations teams are not completely separated. Usually in DevOps, the security and quality teams are more integrated with the development lifecycle. In an article about DevOps it was said that when making "quality deliveries with short cycle time", it needs a lot of automation (Ebert et al., 2016).

DevOps can be identified as the combination of certain practices, tools and philosophies, which enlarge an organization's application and service delivery velocity. It allows organizations to improve their products at a rapid pace. The benefits of DevOps compared to traditional Software development lifecycle are speed, reliability, rapid delivery, scalability, collaboration, and security. The main practices of DevOps are continuous integration, continuous delivery, infrastructure as a code, microservices, monitoring, logging, communication, and collaboration. Integrating DevOps into an organization's practices usually means that the "DevOps culture shift" must be done. This means some of the old practices should be forgotten, like a siloed culture of development and not collaborating. (Ebert et al., 2016)

2.4 DevSecOps

DevSecOps (development-security-operations) is created to help to shift the security processes to left with DevOps. The idea is to integrate security as early as possible in the implementation and design of projects. Security is one of the fundamental parts of the DevOps cycle. A lot of the DevSecOps security can and should be automated, but threat and risk assessment along with a few other security activities cannot be automated yet. (Rahman and Williams, 2016)

Normally in the software development lifecycle, security is managed at a later stage of the cycle. The shift-left security and continuous security assessment are the most important practices of DevSecOps. (Rajapakse et al., 2022) DevOps has been positively impacting software security, by using automation to help with monitoring, deployment, and testing. In addition, software delivery in smaller increments has been found to help with security (Rahman and Williams, 2016).

On the contrary, some studies show the integration of security into DevOps has been a challenge for many organizations (Rajapakse et al., 2022). There have been some activities that have been found to make security in DevOps more difficult, like using inappropriate software metrics (Rahman and Williams, 2016). It has been also stated that continuous delivery would not ease making safety-critical systems (Ebert et al., 2016).

3. THREAT AND RISK ASSESSMENT

There are two types of processes this thesis studies: risk analysis and threat modeling. Risk analysis and threat modeling are slightly different, but the main idea is to find risks and threats so that they can be eliminated.

The risk assessment process should establish and maintain information security risk criteria. It should confirm that "repeated information security risk assessments" result in "consistent, valid and comparable results". It should identify, analyze, and evaluate the risks. (ISO Central Secretary, 2017) According to ISO 27000, risk assessment shall cover risk analysis and risk evaluation. Risk analysis is for estimating the magnitude of risks and risk evaluation for determining the seriousness of the risks (ISO Central Secretary, 2020). The analysis can be qualitative, quantitative or a mixture of these two (ISO Central Secretary, 2019). Qualitative analysis can be easier to do, but it doesn't tell the financial benefits of eliminating risks (Cronk and Shapiro, 2021). The output of qualitative analysis can be presented with numbers, that tell just an approximate idea of the risk level.

Threat modeling should be able to identify high-risk threats. Threat modeling is not recommended to be done by automation; it should be done with the team. Threat modeling techniques are mostly qualitative. (Rahman and Williams, 2016)

In the table 3.1, there is an example of qualitative risk analysis matrix. The risk impact results are multiplications of consequences and likelihood. The results are rated as low (1-3), medium (4-9), high (10-15) and very high (16-20). This is just an example on how the impact of the risks can be presented.

Table 3.1. *Qualitative analysis matrix example.*

		Consequences				
		Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Likelihood	Very High (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	Very Low (1)	2	3	3	4	5

When organizations integrate these assessment processes, it can limit the risks of software-based systems (Maheshwari and Prasanna, 2016). ISO 27000 states that the assessments should be done "periodically" and when "significant changes occur" (ISO Central Secretary, 2020).

There are multiple different methods of risk and threat assessments available. In this thesis, the concentration is on a few well-documented methods, as well as newer CTM-method, as it gives insightful information for continuity of the assessments. Information security assessment for DevOps is recommended to be continuous. The problem here seems to be the lack of general agreement on how security measures should be included in DevOps and its pipelines. (Rajapakse et al., 2022)

3.1 ISO 27005

ISO 27005 provides guidelines for information security risk management. This standard gives an overall view of the risk assessment process, and doesn't necessarily give very detailed rules but is more of a guideline. (ISO Central Secretary, 2019)

Risk assessment consists of risk identification, risk analysis and risk evaluation. The first step of risk identification is to identify the assets. They can be divided into two groups: primary assets (business processes and activities) and supporting assets (hardware, software, network, personnel, site, and organization's structure). The next step is to identify the threats and existing controls. The identification of the existing controls is made to make sure that the controls are working how they should be and to avoid unnecessary work later in the assessment. The following step is to identify all the vulnerabilities, and after that the consequences. (ISO Central Secretary, 2019)

Risk analysis can be done qualitatively, quantitatively or using a mixture of both. Usually, a qualitative analysis should be done first, and if needed, then a quantitative analysis can be done. After choosing the form of analysis, the organization must assess the consequences. The consequences can be shown in technical or human impact criteria, or other criteria that fit the organization. The next step is to assess the incident likelihood in qualitative or quantitative form. The organization should also find the level of risk determination. (ISO Central Secretary, 2019)

In risk evaluation step, the goal is to prioritize risks about the incident scenarios that lead to those risks. The organization should also agree on a scale to be used in the whole organization. It is normal to use any levels between 3 (e.g., low, medium, high) and 10. The table 3.1 uses the level 5 as an example. As a result of the ISO 27005 risk assessment, the organization will have lists of assets, threats, controls, vulnerabilities, consequences, the likelihood of incident scenarios and a list of risks prioritized. With this information, the organization can start to implement their risk treatment process easily. (ISO Central Secretary, 2019)

ISO 27005 is made for organizations, but it does not define whether it is suitable for DevOps organizations or not.

3.2 CORAS

The CORAS method is an asset-driven defensive risk analysis. The CORAS Approach consists of a customized language, a tool, and a method. In this thesis, the focus is on the CORAS method. The method is divided into 7 steps. The first step is to have an introductory meeting. In the meeting, the representative of the client presents the goals of the analysis. The second step is a meeting where analysts will share their understanding and the high-level security analysis is done. In the third step, there is a more in-depth of the analyzed target. The next step is to have a workshop, where the goal is to identify potential undesired incidents, vulnerabilities, threats, and threat scenarios. (den Braber et al., 2007)

The fifth step is another workshop, where the idea is to estimate the consequences and likelihood of the incidents identified in the fourth step. In the next step, the client is given the first general risk picture. The last step is focused on treatment identification, and it can be done as a workshop. The costs and benefits related to treatments are also discussed. (den Braber et al., 2007)

CORAS is a heavy risk analysis due to its multiple steps, and it requires a lot of business hours. It was not associated with DevOps in any of the studies this thesis researched.

3.3 OCTAVE

The OCTAVE methodology comes from the words Operationally Critical Treat, Asset, Vulnerability and Evaluation. It is a qualitative methodology often used for its flexibility. The OCTAVE is made for over 300 employee companies and OCTAVE Allegro can be used in small to medium organizations. OCTAVE-S is created specifically for smaller companies. In the OCTAVE methodology, there are three phases with several processes. (Gunawan et al., 2011)

The first phase of OCTAVE and OCTAVE-S is for building asset-based threat profiles. The important asset, security practices and vulnerabilities are identified. The second phase is for identifying infrastructure vulnerabilities, which could damage the assets. The last phase is to develop a security strategy and plans. The security risks are removed or mitigated, and risk profiles are created. The organization should create a plan to protect the assets. The scale to determine risk probability is often very high, high, normal, low and very low. (Alberts et al., 1999)

OCTAVE Allegro is a more lightweight version of OCTAVE. It starts with preparation, where the risk measurement criteria are established, an asset profile is made and information asset containers are identified. The second phase is similar to normal OCTAVE, it is where the asset profiles are developed. Next, the information asset containers need to be identified. The last phase is threat identification. All these phases are then divided into two steps each. (Alfarisi and Surantha, 2022)

All three methods are relatively similar. When performing the analysis, the OCTAVE method needs a workshop that the analysis team attends. In OCTAVE-S analysis team is formed from 3-5 people who have large-scale knowledge of the organization. OCTAVE Allegro is more flexible, and it can be performed by individual employees or in workshops, where many teams participate. (Alfarisi and Surantha, 2022)

None of the OCTAVE methods was connected to DevOps in the studies that this thesis research. Octave allegro was said to be easy to adapt to various kinds of environments, for example, a cloud environment (Alfarisi and Surantha, 2022).

3.4 FAIR

The Factor Analysis of Information Risk is a quantitative method to analyze information security risks. It is the only fully quantitative method analyzed in this thesis. There are two types of FAIR methods; FAIR, which is made for organizational risks, and FAIR-P, which addresses privacy risks to individuals. FAIR divides risk into factors that can be used to approximate risks from emerging risks. (Cronk and Shapiro, 2021)

FAIR provides a risk taxonomy that separates into 12 specific factors. Each factor contains loss and probability calculations. In table 3.2 there is an example of the outcome of FAIR analysis. The table does not include all of the values that are generated in FAIR analysis, just few examples: primary response, secondary response and secondary fines. The values are examples and not any company's real data.

Table 3.2. *Quantitative FAIR analysis example.*

Loss Type	Min.	Most Likely	Max.	Confidence
Primary Response	3000 €	9000 €	20 000 €	Moderate
Secondary Response	1000 €	10 000 €	50 000 €	Moderate
Secondary Fines	0 €	0 €	2 000 000 €	Low

FAIR-P uses a scale to rank the severity of the privacy harm. It also combines the harm with the risks of substantial harm coming from the fundamental risk. This means that all quantifications used in FAIR-P are using a theoretic model based on empirical data. The advantage of FAIR relies on the numbers: the outcome of FAIR analysis can be for example that with a control costing x euros the company can reduce the annual risk by y euros. (Cronk and Shapiro, 2021)

The FAIR method was not connected to DevOps particularly in the studies that this thesis analyzed. It is very precise and heavy analysis.

3.5 STRIDE

STRIDE is a qualitative threat modeling type, It is developed by Microsoft, and is often used in Microsoft Security Development Lifecycle. It splits threats into six categories, which are spoofing tampering, repudiation, information disclosure, denial of service and elevation of privilege. The threat modeling process starts with identifying assets and creating an architecture overview, for example with data flow diagram. Then the application should be decomposed to create a security profile for the application. After that, the organization should identify the threats, and finally rate the threats to prioritize them. There is a formula that helps to indicate the risks: Risk = Probability x Damage potential. (Microsoft, 2010)

The organization can use a 1-10 scale for the probability of the threat occurring. There should be a similar scale for damage potential, from minimal damage (1) to catastrophe (10). Then probability and damage potential are multiplied together, a number between 1 to 100 is created, and we can divide it into a scale for low, medium, and high-risk ratings. (Microsoft, 2010)

STRIDE is found to be easy to do, but there are study results that state its time cost is relatively large. The researchers have found out that the number of overlooked threats was very high and there were also incorrect, unnecessary threats found. (Scandariato et al., 2013)

DREAD is sometimes done with STRIDE. It helps to determine what is the likelihood of the STRIDE threats happening. DREAD is divided into five parts: damage potential, reproducibility, exploitability, affected users and discoverability. These are rated by 1-3, high, medium and low ratings. The organization can now go through each threat found in the STRIDE method, and rate them by DREAD. Each of these DREAD ratings will be added up to a total number, where 5-7 represents low risk, 8-11 medium risk and 12-15 high risk. After the risk rating is done, the organization needs to update their documented threats to add the rating level (Microsoft, 2010).

Threat modeling and especially STRIDE has been mentioned as one of the assessment type options for DevOps.

3.6 CTM

Continuous Threat Modeling (CTM) is Autodesk's qualitative threat modeling methodology that helps development teams perform threat modeling with less dependency on security experts. The idea of this methodology is to bring security closer to all the team members so it would be easier to perform and update. In this model, it is thought that everyone on the development team should have a stake in threat modeling. Of all the methods introduced in this thesis, CTM is the least strict method, meaning that it states that there is "no ’right’ way to performing a threat model". (Autodesk, 2020)

A data flow diagram is also done in CTM to understand the data flow. There are sample questions given for different security subjects, like access control or cryptography. The findings are documented using for example CVSS format. After the first draft of the threat model, a member of the security team should review the completeness of the document. There is also a review process with the stakeholders about threat modeling materials. CTM is recommended for updating when architectural changes are made, deployment requirements changes, code is inherited, new third-party components are added, or authentication or authorization is modified. (Autodesk, 2020)

The process is like normal Threat Modeling; First, the scope is defined, and the important assets are identified. Based on the scope, the diagram can be drawn along with dataflows. It is important to identify where the important data exists and moves. When these steps are done, there are subjects like Access Control or Trust Boundaries with questions to help with the threat modelling. The questions are there to help developers and other employees to have the right security mindset for the assessment. In the end, the findings need to be documented. The idea after this is to keep the threat model updated. (Autodesk, 2020)

There is not too much documentation about CTM, so it must be used with consideration. CTM is generally bringing the Threat Modeling "to the left", which aligns with DevOps processes and the culture overall.

4. RESULTS

The different assessment processes have slightly different steps, but the overall process seems to fit within the common phases: risk/threat identification, risk/threat analysis and risk/threat evaluation. The definition of the project or the scope is important to understand at first, that the protected assets are identified. Risk analysis and threat modeling are primarily done to find out what assets needs protection from which risks.

It has been studied that a lack of tools and methods for information security assessments for DevOps could get in the way of performing the assessments (Rajapakse et al., 2022). There are no exact information on compatibility for DevOps and some of these methods. DevOps is known for its speed, rapid delivery, scalability, collaboration, and security. When deciding on the best threat and risk assessment method for DevOps, these factors need to be considered.

There doesn't seem to be a straight answer to what is the best way to do risk and threat assessment for DevOps. The assessments presented in this thesis have some similarities and some differences. Some factors could make the assessment more difficult to make. One of these is quantitative analysis types because it might be difficult to revisit quickly unless there is a clear idea of the quantitative losses. One option is to do quantitative risk assessments at the higher levels of the organization. If the assessment method is too heavy, it might be difficult to revisit and doesn't align with DevOps' speed.

In a study comparing different risk assessment methods, ISO 27005 was found to be the most complete approach when comparing it to the Core Unified Risk Framework. This is only one approach, and it does not consider the specialities of DevOps. However, the study shows that ISO 27005 is superior in risk identification and risk estimating completeness. The standard is more of an overall risk assessment method, and this makes it adaptable for many kinds of organizations. ISO 27005 states that risk analysis can be qualitative, quantitative or both. (Wangen et al., 2017) This could give the organization the freedom to choose the right analysis type. It is difficult to analyze ISO 27005's speed or the ability to scale or be collaborative because there can be many ways of doing it. ISO 27005 shows signs of good assessment type, because of its convertibility and completeness.

The second highest ranking in the study comparing the methods was for FAIR (Wangen et al., 2017). The FAIR method is quantitative, and it needs a lot of information from experts. Things like privacy information loss can be sometimes difficult to quantify. The method also needs many steps to complete. That can make it difficult for the DevOps teams to revisit quickly. The positive side of FAIR is its exactness with numbers and the ability to show a quantitative loss.

The CORAS method needs a lot of steps to complete, which makes it a heavy risk assessment process. In field trials done for the method, there were about 250 business hours used from the analyst side and less than 100 hours from the client. This could make it difficult to update and doesn't align with DevOps' speed and rapid delivery. Because of the large number of hours needed it might also be difficult to scale the assessment easily. It was also lacking on risk estimation (Wangen et al., 2017). In reverse, CORAS does have a lot of workshops organized and that makes it necessary to collaborate, which aligns with DevOps. (den Braber et al., 2007)

The OCTAVE method is done for a small team within a large organization. This could make it suitable for large organizations with a lot of small DevOps teams. OCTAVE-S is for an organization that is small and has a simple or flat hierarchy. OCTAVE methods require some expert knowledge to complete them. Octave Allegro was said to fit within multiple organizations and various environments. It is also a more flexible analysis, doesn't require broad knowledge about risk assessments and is not as heavy as OCTAVE or OCTAVE-S. This could make OCTAVE allegro the most suitable type for DevOps out of the three OCTAVE methods. (Alfarisi and Surantha, 2022, Alberts et al., 1999, Gunawan et al., 2011) The Allegro was also ranked high when it comes to completeness in the CURF study (Wangen et al., 2017).

Threat modeling in general is brought up several times as an option for DevOps' security assessment. Threat modeling got little more attention in a DevOps security conference than risk analysis, although risk analysis was used more (Rahman and Williams, 2016). STRIDE was mentioned to be one of the threat modeling types to identify vulnerabilities in the DevOps CD pipeline (Georgeta and Alexandru, 2017). STRIDE is often done in teams, and it makes it collaborative. However, there was evidence that found that although STRIDE is easy to do, it is not always fast to do. It can also produce an overwhelming number of threats and that might make it more difficult to find out the most important threats. (Scandariato et al., 2013)

When thinking about DevOps' continuous delivery, the Continuous Threat Modeling (CTM) could fit within the DevOps lifecycle and culture (Autodesk, 2020). There are not yet studies on CTM, although it seems to bring together threat modeling in a more accessible way. Continuity does not mean that the team organizes a workshop whenever a new commit is added. It would mean revisiting and updating the threat model when new events come up. CTM is not necessarily light, but its purpose is to make threat modeling simpler, easier to update and more collaborative. It is also supposed to be easy to revisit and offers questions to help with the revisiting process. (Autodesk, 2020) Because of the lack of studies on CTM, it should be looked at and used with caution.

As seen here, all the studied methods had positive and negative sides.

5. CONCLUSION

This thesis studied different types of threat modeling and risk analysis techniques and how they fit with DevOps. The best way to do threat and risk assessments for DevOps could be some sort of continuous assessment with some collaboration, regarding on what assessment type the DevOps team decides to use. The assessment should be easy to update and most importantly, it should be done.

ISO 27005 was found to be a good overall method that can be modified to fit the organization's needs. There need to be more studies on its compatibility for DevOps, but the methods seem to be adaptable. FAIR was found to be accurate but lengthy and difficult to do because of its quantitativeness. CORAS shows signs of heaviness but its positive side is collaboration. OCTAVE methods, especially OCTAVE allegro had good flexibility, but normal OCTAVE needs an analysis team from business units to conduct the analysis. STRIDE had good collaboratively and is easy to do but can be heavy and produce unnecessary threats. CTM didn't have studies behind it, but it seems to bring together continuity, collaboration, and easiness.

As analyzed in the results, there is no plain truth for what is the best information security risk and threat assessment method for DevOps. There are very promising factors in some assessment types, like continuity in CTM, but with the studies done, there is no hard truth. Some factors, like the heaviness of the process or quantitative methods, might be in the way of revisiting the assessments.

An organization could perform risk or threat assessments in an alternative way. They could take the assessment model that fits their organization best as a guideline. After that, they could get the idea from the CTM, which is to shift the process left. The DevOps team could revisit their assessment or model every time some changes are made in the architecture or something new is added. This would ensure speed and rapid delivery. In addition, working as a team, which means collaborating is one of the DevOps principles. This would bring the best qualities of all the methods together, and make them more suitable for DevOps processes.

If the threat modeling and risk analysis process could be perfect and easy, it would be automated already. Risks are not always too easy to define, and sometimes humans make mistakes that lead to security problems. The most important thing in my estimation would be to get the assessment done and updated. The results of the assessments should be used to mitigate negative security incidents and to improve overall information security, regardless what type of assessment is used.

There is still a lot of work to do in the DevSecOps field and getting security to be a more integrated part of DevOps. The importance of security measures should be emphasized in the future. The suitable way of performing threat and risk assessment for DevOps should be studied more to get more precise results. Automation is important part of DevOps, and integrating it to risk and threat assessments somehow could ease the processes in the future.

REFERENCES

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0*.

Alfarisi, S., & Surantha, N. (2022). Risk assessment in fleet management system using octave allegro. *Bulletin of electrical engineering and informatics (edisi elektronik)*, *11*(1), 530–540.

Autodesk. (2020). *Continuous threat modeling*. Retrieved September 27, 2022, from https://github.com/Autodesk/continuous-threat-modeling

Cronk, R. J., & Shapiro, S. S. (2021). Quantitative privacy risk analysis. *2021 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROSPW 2021)*, 340–350.

den Braber, F., Hogganvik, I., Lund, M., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps - a guided tour to the coras method. *BT technology journal*, *25*(1), 101–117.

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). Devops. *IEEE software*, *33*(3), 94–100.

Georgeta, P. N., & Alexandru, P. C. (2017). Risk assesment: An important tool for companies. *Global economic observer*, *5*(2), 97–102.

Gunawan, B., Merry, M., & Nelly, N. (2011). Information technology risk assessment: Octave-s approach. *CommIT (Communication and Information Technology) Journal*, *5*(1), 1–4.

ISO Central Secretary. (2017). *Information technology. Security techniques. Information security management systems. Requirements* (Standard). International Organization for Standardization.

ISO Central Secretary. (2019). *Information technology - Security techniques - Information security risk management* (Standard). International Organization for Standardization.

ISO Central Secretary. (2013). *Industrial communication networks. Network and system security. Part 1-1 Terminology. concepts and models* (Standard). International Organization for Standardization.

ISO Central Secretary. (2020). *Information technology. security techniques. information security management systems. overview and vocabulary* (Standard). International Organization for Standardization.

Maheshwari, V., & Prasanna, M. (2016). Integrating risk assessment and threat modeling within sdlc process. *2016 International Conference on Inventive Computation Technologies (ICICT)*, *1*, 1–5.

Microsoft. (2010). *Threat modeling*. Retrieved September 27, 2022, from https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN#c03618429_011

Rahman, A. A. U., & Williams, L. (2016). Software security in devops: Synthesizing practitioners' perceptions and practices. *INTERNATIONAL WORKSHOP ON CONTINUOUS SOFTWARE EVOLUTION AND DELIVERY, CSED 2016*, 70–76.

Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting devsecops: A systematic review. *Information and software technology*, *141*, 106700–.

Scandariato, R., Wuyts, K., & Joosen, W. (2013). A descriptive study of microsoft's threat modeling technique. *Requirements engineering*, *20*(2), 163–180.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness: Core unified risk framework, curf. *International journal of information security*, *17*(6), 681–699.