jamk

Enhancing incident management process

Eetu Kettunen

Master's thesis
May 2023
Information technology
Master's degree programme in Cybersecurity

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Kettunen, Eetu

Enhancing incident management process

Jyväskylä: JAMK University of Applied Sciences, May 2023, 76 pages.

Information technology, Master of engineering in information technology, cyber security, Master´s thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Incident management process is an important part on enabling the organization's ability to be efficient on resolving occurred security incidents. Incident management process defines important aspects and serves as guideline on how to act during a security incident. There are many guidelines and frameworks on building a proper incident management process, but none of those are universal and must be tailored for each need in different organizations.

The research began with literature review about security incident management subject, which then served as a base for reviewing the security incident management process in use. Data was gathered in addition to previous research and literature, also with questionnaire that was sent to selected individuals who work within the field of cyber security in different ways.

This research aims to enhance a security incident management process that already exists, by reviewing existing documentation as well as conducting structured interview for personnel working with cyber security. The questions were formed to gain insight on how well personnel is familiar with the current security incident management process and gain firsthand knowledge on development needs on that same process.

In addition to security incident management process, secondary objective for this research is to find required skills for forming well-functioning virtual security incident response team. Questionnaire was used to gain recommendations and observations on what skills were thought to be necessary or possibly missing in the current situation.

The results are then presented in a suggestive manner, due to upcoming organizational changes. Organization is undergoing a fusion process, results can be used during different phases of the organizational changes to help build well-functioning security incident management process, as well as form a new virtual security incident response team.

Keywords/tags (subjects)

Cybersecurity, incident management process, security incident response team

Miscellaneous (Confidential information)

-

jamk

Kuvailulehti

Kettunen, Eetu

Tietoturvapoikkeamien hallintaprosessin tehostaminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2023, 76 sivua.

Tekniikan ja liikenteen ala. Insinööri (ylempi AMK), tietotekniikka. Master's Degree Programme in Information Technology, Cyber Security. Opinnäytetyö YAMK. Julkaisun kieli: Englanti

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tietoturvapoikkeamien hallintaprosessi on tärkeä osa organisaation kykyä ratkaista tapahtuneet tietoturvaloukkaukset tehokkaasti. Prosessi määrittelee oleelliset osa-alueet ja ohjeistaa miten tietoturvapoikkeamien aikana tulisi toimia. Asianmukaisen hallintaprosessin muodostamiseen on olemassa monia standardeja sekä viitekehyksiä, mutta nämä käsittelevät aihetta vain yleisellä tasolla eivätkä ole yleispäteviä, vaan prosessi tulee räätälöidä vastaamaan jokaisen organisaation omia tarpeita.

Tutkimus aloitettiin tietoturvapoikkeamien hallintaprosessiin liittyvällä kirjallisuuskatsauksella, joka toimi pohjana, kun tarkasteltiin organisaation nykyisesti käytössä olevaa tietoturvapoikkeamien hallintaprosessin dokumentaatiota. Tietoa kerättiin kirjallisuuskatsauksen lisäksi myös haastattelemalla organisaation sisältä sopivia henkilöitä, jotka työskentelevät tietoturvan parissa eri tavoin.

Tutkimuksen tavoitteena on tehostaa olemassa olevaa prosessia tarkastelemalla dokumentaatiota, sekä keräämällä tietoa mahdollisista ongelmista kyselyn avulla. Kysymykset laadittiin sitä silmällä pitäen, kuinka hyvin henkilöstö tuntee käytössä olevan prosessin, sekä saada tietoa käytännön kokemuksiin pohjautuvia tietoja prosessin kehitystarpeista.

Toissijainen tavoite tutkimuksessa oli selvittää virtuaalisessa tietoturvatiimissä tarvittavat taidot, nämä taidot koostuivat sekä teknisistä, että ei teknisistä taidoista ja kyvyistä. Haastatteluista saatiin ajatuksia siitä, minkälaisia taitoja arvostetaan tai vaaditaan onnistueen tiimin kasaamisessa.

Tulokset esitetään suosituksina, sillä organisaatio on läpikäymässä suuria organisaatiomuutoksia, joten tuloksia ei voida suoranaisesti ottaa heti käyttöön, vaan tuloksia voidaan käyttää myöhemmissä vaiheissa organisaatiomuutosten aikana. Tuloksia voidaan käyttää auttamaan siinä vaiheessa, kun organisaatiomuutokset ovat siinä pisteessä, että uusia tietoturvaprosesseja on aiheellista miettiä siirtyneille osakokonaisuuksille.

Avainsanat (asiasanat)

Vianhallinta, tietoturva, häiriöiden käsittely

Muut tiedot (salassa pidettävät liitteet)

-

Contents

1 Introduction 6
2 Overview of the research 7
2.1 Research problem 7
2.2 Research questions 8
2.3 Previous research 8
2.4 Constructive research approach 10
2.5 Goals 11
3 Theory 13
3.1 Security incident management 13
3.2 Security incident response team 17
4 Questionnaire 21
5 Analyzing the data 22
5.1 Security incident management process 22
5.1.1 Awareness of process 23
5.1.2 Development needs 24
5.2 Security incident response team 26
5.2.1 Awareness on what Security Incident Response Team (SIRT) is? 26
5.2.2 Determining on what skills are valued for SIRT 27
6 Conclusions 30
6.1 Results for security incident management process 30
6.2 Results for security incident response team benefits 32
7 Reflections 33
7.1 Ethics 33
7.2 Thesis process 33
7.3 Possible future research 34
References 35
Appendices 38
Appendix 1. P1 Transcript 38
Appendix 2. P2 Transcript 42
Appendix 3. P3 Transcript 47
Appendix 4. P4 Transcript 53
Appendix 5. P5 Transcript 61
Appendix 6. P6 Transcript 66

Appendix 7. P7 Transcript 69
Appendix 8. P8 Transcript 73

Figures

Figure 1 Incident response process (Adapted from Research and Management Security Incidents 2018.) 17
Figure 2 SIRT workflow (Adapted from Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams 2014) 20
Figure 3 Simplified security incident management process 23

Tables

Table 1 Development needs by participants 25
Table 2 Development need percentages by participants 25
Table 3 Skills given by participants 27
Table 4 Percentages of repeated skills 28

1 Introduction

The purpose of security incident management process is to guide personnel through occurred security incident. This means that the process should be documented clearly, but at the same time it should be simple enough for anyone to understand it. Security incident management process should be working in a way, that occurred incidents can be resolved in a hastily manner and learn from the incidents that have been solved. Just like any other process inside the organization, security incident management process also requires constant developing and updating for it to answer the needs that future is throwing at it.

The bases of security incident management process are very simple, but the variation comes that some sections of that base process description require more attention than the others in different organizations, based on their needs and functions. The roles of participants in security incident management process should be clear to anyone who are part of it, and to those who need to report incidents, without that, the incident management process cannot work properly and there will be stand stills and possible even incidents that aren't being reported.

This thesis goes through security incident management process, with the addition of researching the needed skills in a virtual security incident management team. Especially the security incident management process subject is well known topic and has a lot of studies done to it and relies heavily on 3 major standard or framework, ISO/IEC 27000-series, NIST CS800-series and ITIL framework.

The purpose of this work is to go through organizations security incident management process documentation, conduct a structured interviews with suitable personnel and perform analysis on what steps should be taken in order to enhance the security incident management process. Second part of this thesis focuses on finding the needed skills in order to form a well-functioning virtual security incident response team (SIRT).

2 Overview of the research

This chapter goes through the overview of this research, what is the research problem at hand, what are the research question and what kind of previous research has been conducted regarding this topic. This section also answers on method chosen for research approach as well as the goals of this thesis.

2.1 Research problem

The problem to be addressed by this thesis is that the current security incident management documentation can be confusing and hard to understand when opening the documentation for the first time. This is because that the documentation has implementation of two different security incident management documentations from two different organizations. Both documentations were developed and implemented in their own companies, but after companies merged, these documentations were put together into one and in certain areas, the quality of the documentation has suffered due to the swift schedule. In addition to this, teams that are working with security incidents might have their own processes to deal with reported incidents. Overall, this security incident management process includes all the needed steps in order to comply the ISO 27001 standard, but the process charts and documentation has been left a bit short or they haven't been updated in years. Documentation is combination of Finnish and English and should be unified in the future so the documentation would be more formal.

This situation is caused by the requirement of ISO 27001 certified partner in some customer projects, this caused documentation to be developed in a switch manner due to time limitations for the external audit process. Same process went through in another company, which at later stages was merged together with the first company, and these documents were then merged into one. Now during this thesis, the object is to review this whole documentation and create suggestions based on the problems discovered during the review and interviews that would result in better process for the incident management.

Initially the purpose of this thesis was to review organizations current documentation status, how the process is working and create enhanced version of this process. However, due to changed atmosphere within the organization, which means that the organization started another migration

process after the thesis work was already started, this thesis now looks to identify major problems in this current situation and make suggestions based on those identified problems on how to enhance this security incident management. Second problem that this thesis is looking into is to find answer on what requirements for well-functioning security incident response team there is. What are the needed skills for SIRT and what its capabilities are. These results are then given in a suggestive manner, which then will be used during the different phases of that change management process that the organization is going through.

2.2 Research questions

The objective for this thesis is to answer following questions:

- How can proper incident management improve efficiency of solving incidents?
    - Literature review aims to find answer to this.
- What are the main areas that require developing within the organization?
    - Conducting structured interview to find those development needs.
- What are the benefits of using virtual response teams?
    - Literature review to find benefits of virtual response team.

2.3 Previous research

There has been quite a lot of previous research on this topic, most of them seem to rely heavily on ISO 27000-series standards, as well as ITIL4. Most of the research is scoped into some specific business areas, but the same principles are still there. Because every environment is different, some adaptations are to be made in every organization security incident management process that works best for the organization in question.

In his master's thesis Mika Haapakoski (2018) researched incident management process inside multi-vendor environments. That research used tools from ISO/IEC 27001 standard as well as VAHTI and Katakri for creating a survey for interviewing suitable customers.

Tanja Ruskojärvi (2020) generated security incident management process in network operation center (NOC) and tested the processes in laboratory environment as well as created a plan for continuous development. Ruskojärvi's goals was to create a procedures and processes that are functional and achieve sufficient capabilities to respond to security incidents.

In their study Line et al. (2014) they investigated on how security incident management has been performed in organizations that are operating in power industry. Their research view was to find out how those organizations have been prepared and planned activities for security incident management, as well as what differences there are between IT systems and Industrial Control Systems (ICS).

There was also a study conducted for the field of power industry, this study was about adopting security incident response team (SIRT) for proper security incident management in Smart Grids. de Jesus Martins et al. (2019) studied the requirements for specialized SIRT that must be capable for handling the physical infrastructure, smart grid equipment as well as the IT infrastructure.

Daniel Cullen (2019) studied the required skills and characteristics for SIRT in a qualitative manner, he focused more in finding the skills required to perform in virtual team. He conducted a survey where he identified required set of skills that could be used in large organizations to ensure that all the found skills are present in their virtual security incident response teams.

These studies are just a few to mention that were discovered during the literature review process, there were many studies conducted in different fields, but the bases are all the same no matter where the study was conducted for.

2.4 Constructive research approach

This section goes through why this research approach was chose and how is this method being used.

Constructive research approach can be categorized as applied studies which often ends with new knowledge and views on the subject that was researched. This method is used to define and solve problems in addition to improve already existing systems or processes with adding the already acquired knowledge base to the theoretical research (Oyegoke 2011).

Constructive research approach was initially developed for research in management accounting but is widely used in management information systems as well as logistics and project management. Constructive research approach tries to find a balance between practical problem-solving with professional experience and potential theoretical contributions. Constructive research approach involves three phases, which are:

1. preparation
2. fieldwork, and
3. theorizing (Jones et al. 2022).

Due to the nature of this research, constructive research approach was a natural selection to select. Data collection was done by reading the current security incident management documentation and interviewing personnel working in cyber security. Interviews were held after obtaining a general level understanding of the current status.

Work began with reviewing literature around the themes of security incident management and security incident response team. After enough material was gone through, then followed the getting to know the status of organizations security incident management process in use. After familiarizing current security incident management process, questionnaire for the structured interviews was thought in collaboration with thesis counselor from organization. Questions were divided into two different themes, first theme was built to gain knowledge on security incident management process, how well the process is known between the specialists that work with cyber security, as

well as find possible development needs within that process. Second theme was built around security incident response team (SIRT) and the questions were formed to gain understanding on how well the SIRT concept is understood within the organization, as well as find out what kind of skills are thought to be useful and needed in order to have a well-functioning SIRT.

After the questions that could benefit this research were formed, invitations for suitable personnel were sent. Initially there was eight (8) persons selected, one person had to decline due to time limitations, but this person also provided suitable person to take part of the interview instead. Finally, after interviews were held, data gained from those interviews were analyzed and suitable recommendations about the improvements were given.

2.5 Goals

The goal of this thesis was originally to enhance current security incident management process, so that problems identified during the interviews can be resolved. The plan was initially to review current status of the security incident management, conduct an interview with the personnel that are working in one way or another with the cyber security and find out the problems that lie inside that security incident management process. After the problems have been identified, then the idea was to update the incident management process to resolve the identified issues.

However, due to circumstances that could not have been foreseen, the company that commissioned this thesis, started a change management process in which it is merging into two different companies, the implementation part of this thesis was then dropped out. The implementation phase would not beneficial to the organization, as the organizational structure is about to change and new processes has to be constructed.

This thesis focuses to identify on problems that lie in the current security incident management process by reviewing the current documentation and conducting structured one-to-one interviews with suitable personnel. Once the documentation has been reviewed and data analyzed from the interviews, give recommendations based on the findings what actions should be taken into consideration during the change management process when services are moved into their new management location and new security incident management process is needed.

Second part of this thesis was to find out the characteristics and skills needed for the well-functioning virtual security incident response team; these requirements were studied from the previous research about the subject as well as gathering data from the interviews that was conducted during this research.

3 Theory

This part introduces the theoretic background that is relevant to research subject. Theory is divided into two main subjects, security incident management and security incident response team (SIRT).

The source of information relies heavily on International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards, as the company that has ordered this master's thesis has obtained and audited accordingly on ISO/IEC 27001 standard. This means that requirements that are set in ISO/IEC 27001 standard will have to be met, so that company still fulfils the requirements set on the said standard.

ISO 270xx series standards are specifically made for information security, but these standards and guidelines are not making any recommendations for which products or brands to use in order to fulfil requirements set in the standard (Berger et al., 2020).

Second part focuses on SIRT and some requirements are set from the given organization, which includes that the SIRT should be virtual, instead of being traditional tiered model.

3.1 Security incident management

According to the international standard, ISO/IEC 27001:2022, which is one of the most recognized standard in the field of information security management, defines that information security is maintaining the confidentiality, integrity and availability (CIA) of information.

Onwubiko and Ouazzane (2022) state that incidents can come in many forms and ways; they often come unannounced and need to be contained and controlled accordingly. Even when the incidents are foreseen and expected, the impact of the incident can still cause damage if organization is not well prepared. Preparedness is an important part of incident management. Incident management should be well planned, exercised and rehearsed during the use of incident management policy.

Security incident management is one of the main elements of the information security management system (ISMS) process model (Aleksandrova et al., 2020). The main focus of incident management is to recover the IT services to operational status to its customers from the occurred incident, and that due to sensitive nature of the information, management of security incidents can prove to be a difficult task (Berger et al., 2020).

Line et al. (2014) stated that security incident management process itself covers all the different stages of an incident. While ISO standard is describing process to consist of five different phases, only the first stage is running continuously and later phases are only used, when an incident has occurred. ISO/IEC (27035:2023) describes the five stages as following;

1. Plan and prepare;
2. Detection and reporting;
3. Assessment and decision;
4. Responses; and
5. Lessons learned.

Other guidelines describe the incident management process similar to these five stages, although some of these guidelines may have different number of phases, the main ideas and activities are still included inside the process. Following organizations are the providing the most well-known guidelines in addition to ISO/IEC;

- National Institute of Standards and Technology (NIST),
- The European Union Agency for Cybersecurity (ENISA),
- and SANS institute (Line et al,. 2014).

It should be noted that guidelines and frameworks presented by NIST, Information Technology Infrastructure Library (ITIL), or similar are developed by single organizations, that shouldn't be compared directly with ISO/IEC standards, which are based on international consensus (Line and Albrechtsen, 2016)

Another way of summarizing the lifecycle of an incident could be listed as following: (Manage Engine 2023)

1. Logging the incident.
2. Categorizing the incident.
3. Prioritizing the incident.
4. Assigning the incident.
5. Creating tasks and managing them.
6. Managing SLA and escalations.
7. Resolving the incident.
8. Closing the incident.

Once the incident has been closed, there should be post-incident review that aims to document all the different phases of that occurred incident. This documentation helps to develop the incident management process, as well as it helps teams to prepare in future incidents that have similar aspects to them. This process can be put into a smaller pieces to help answer all the needed questions, especially in a major incidents,

1. Identification of the incident, which aims to answer the questions on how and how, as well as to establish the timeline on how fast the incident was detected and could it have been detected earlier?
2. Communications, this phase aims to find out how fast the information was communicated to the stakeholders, what channels were used and how did the updates were communicated during the different phases of the incident?
3. Structure, this part aims to show on how the SIRT was initially structured, was the initially gathered SIRT sufficient to resolve the incident, if not, then what changes had to be made and why? Could forming the initial SIRT be improved in some way?
4. Utilizing resources, this part tries to show what resources were used during the incident and were they being used in the most optimal way? How fast the resources were utilized, and could that be improved in the future incidents?
5. Process section aims to answer the question on how closely the incident management process was followed during the different phases of the incident? Were there any deviations? Were the SLAs fulfilled?
6. Reporting is the final stage which aims to go through on the documentation of the incident, was there anything left out of that documentation? (Manage Engine 2023).

Another way of this post-incident review is to do lessons-learned session where it could be determined if there are any improvements to be made in the process, could there maybe be a need for new procedures? Is there a need to create new alerts, add or create signatures, maybe some

search parameters to add for automation systems? How did the plans work for the occurred incident? Was there a panic, or could the process be executed like planned? Did the incident show that there is a need for additional training? Having these kinds of lessons-learned sessions will allow organizations to identify tasks that still require updates and can give confidence that the process is working (Death, 2017).

Incident handling process can differ in some parts when comparing to the incident management processes. Security incident handling process could start at the preparation, where organization is developing security incident response capabilities in the form of creating a process that includes guidelines on how to respond to security incidents. Process would then move towards identification phase, where it is determined if an incident occurred. Next step is to contain the incident and prevent it from spreading towards other systems. Fourth phase is removal, where the cause of that incident is removed from the system. Fifth phase is recovery, this means that the service is back to normal operations. Finally last phase for this handling process is lesson learned, which includes documentation on what was done, what worked and was there any issues during the incident, this is crucial as this helps organization to improve their processes and enhance handling similar incidents in the future (Rudzitis and Dorogovs, 2018). This handling process is shown in Figure 1 on the next page.

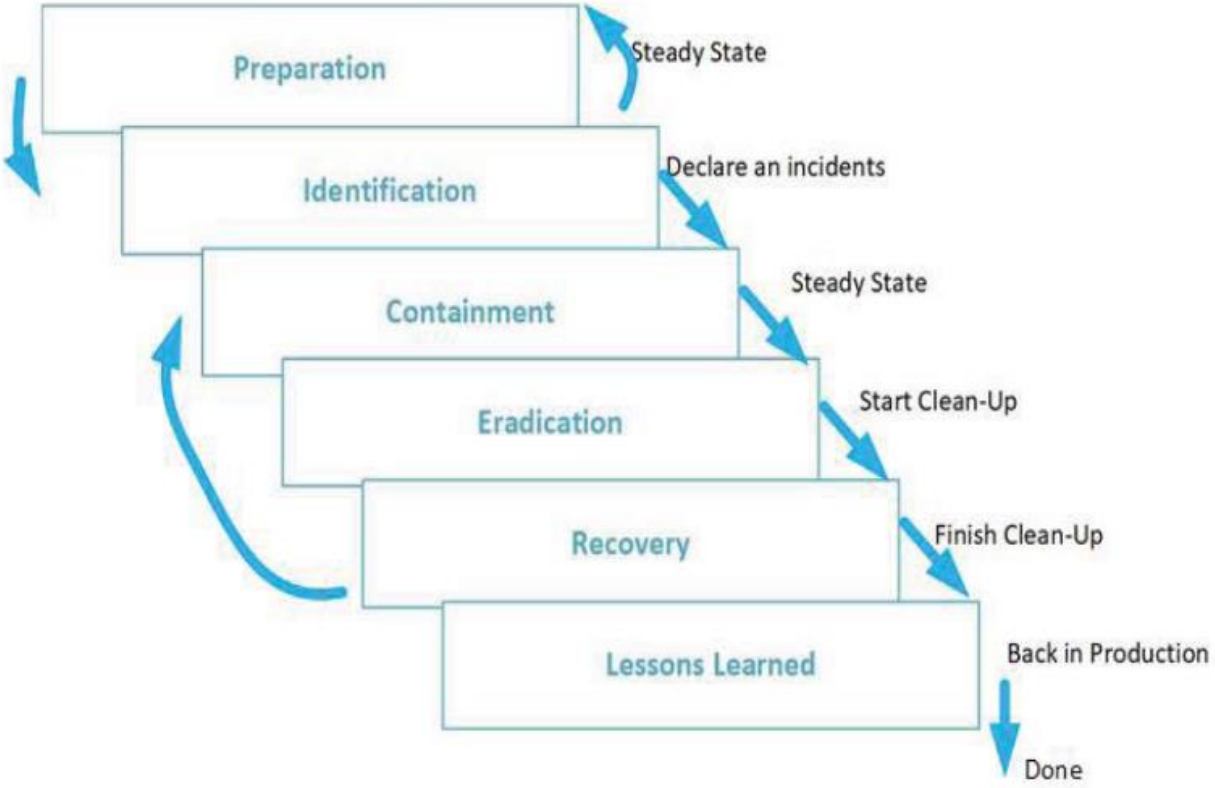

Figure 1 Incident response process (Adapted from Research and Management Security Incidents 2018.)

3.2 Security incident response team

In cyber security, an incident can be described as an event that has a direct or indirect impact on confidentiality, integrity or availability of the system, service or its data. Usually, these occurrences are then handled by company's security incident response team (SIRT). These teams then proceed to work along their organizations documented processes regarding incident management, those processes are there to define every step on how to identify, analyze and resolve security incidents in a fast manner that would reduce the impact and cost of the incident (de Jesus Martins et al. 2019).

In his dissertation manuscript Cullen (2018) wrote increasing amount of threats in cyberspace and the sophistication of those threats has created a need to create an efficient and effective SIRT. This created a need to map out the required skills and characteristics to achieve an effective SIRT. His research reviewed the differences of linear and non-linear SIRTs.

Based on the literature review, the term 'non-linear SIRT' (Cullen, 2018) could also be described as 'swarming' (Boks, 2022), or 'intelligent swarming' (Consortium for Service Innovation, 2022), or 'swarm-intelligence' (Leanne 2021), or even 'virtual SIRT'.

In this thesis I will be using term 'virtual SIRT', which means that SIRT shall operate in different organizational structures, but during the incident shall be working between other debarments and organizations in order to resolve occurred incident (Cullen, 2018).

Swarm-intelligence approach for Computational Emergencies Response Team (CERT) has this idea where agents would gather information from multiple sources and then hand pick the best suitable solutions for different incidents into own databases. The idea behind this is that this way solutions to the problems could already be located inside the organizations database and incidents could be resolved in a much faster pace. This database would grow during its existence and solution database would grow much larger (Aguilar et al. 2009).

According to Red Canary's fifth annual threat detection report (2023) key trending threats in cyber security in the year 2022 were;

1. Ransomware;
2. Initial access tradecraft;
3. C2 Frameworks;
4. Stealers;
5. Identity;
6. Email threats; and
7. Adversary emulation and testing.

Given that the current cyber landscape is constantly evolving, and the malicious actors are developing their skills as well as more sophisticated methods, tools and techniques. The need for combating this has been a well-functioning security incident response team, that has been tasked to take responsibility in receiving, analyzing, and resolving security incidents (Dsouza 2018).

During the corona pandemic organizations moved heavily into working from remote locations, this meant that their activities relied heavily on information technology. This again meant that there was a more uncontrolled use of internet and different services that it provides for its users, this brings more challenges to protect the organizational data, as users are no longer within the organization's IT environment, but still have access to it. To combat these problems, having a security incident response team helps to mitigate and review unwanted actions in the organizations network (Villegas-Ch 2021).

Ioannou et al. (2019) wrote that organizations typically manage and coordinate their incident management processes through SIRT. This team then tries to eliminate, or at least minimize the incident would cause towards the receiving organization. Financial costs could be only on direct side, which means that confidentiality, integrity and availability of information has been compromised, or costs could be more of an indirect cost, like loss of reputation. Organizations should manage to implement proactive and reactive measures against possible incidents.

In large organizations defending their assets usually involve various mechanisms, like different security products and features, such as intrusion detection systems (IDS) which gives alerts when there is suspicious network activity noticed. While automating monitoring as much as possible gives security operators more freedom to work with other tasks, a successful SIRT cannot be successful on automated systems alone, it requires planned and tested workflow that ensures that identified incidents are being handled with correct response. One possible example workflow that was prepared by analysts from the Sandia National Laboratories is shown in Figure 2 (Reed et al 2014).

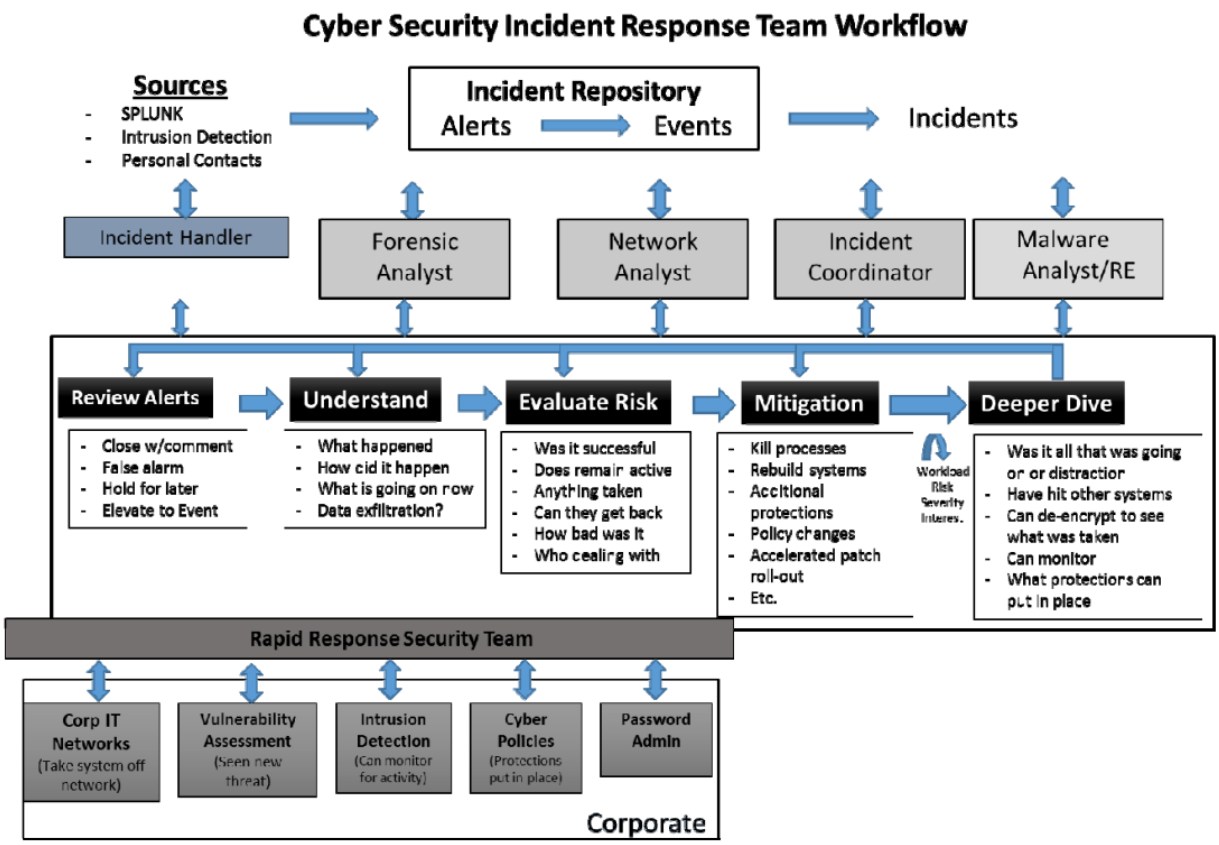

Figure 2 SIRT workflow (Adapted from Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams 2014)

4 Questionnaire

Separated in to two different themes, first part is to gain understanding on current situation, about the problems and how well this current security incident management process is understood with the personnel that are working with this subject. These questions will be sent about one week beforehand to all the recipients, so they have some time to familiarize themselves with the subject if they wish to do so.

The main goal with this questionnaire is to gather some data about the issues in current incident management process that can be then transferred to requirements for the new and enhanced incident management processes and policies as well as the SIRT.

First part of the questionnaire, that focuses on current status of security incident management process includes following questions:

1. Could you describe the different stages that are part of the current security incident management process.
2. Can you name 1-3 stages you think that should be developed more.
    a. How would you put these in order of importance?
3. Please could you tell why you chose these stages in more detail?

Second part of this questionnaire, that focuses on security incident response team includes following questions:

1. How would you define what Security Incident Response Team (SIRT) is?
2. Which needs could be addressed by having a Security Incident response team?
3. What skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

The results of this questionnaire are anonymized, and only general level of the participant background will be included in the results.

5 Analyzing the data

This section presents the findings from the questionnaire. The transcripts of the interviews can be found in the appendices for further research. The participants for this questionnaire were selected based on their participation in the field of cyber security in one way or another. Participants are working in different areas of the organization, from the first response to management level. Interviews were held in Finnish and during the literation the transcripts were translated to English as well as they were anonymized.

The questions were sent beforehand attached to the meeting invitation, so the participants had the possibility to get to know the questions if they so choose, though this wasn't a requirement for the interview. The number of participants who familiarized the questions in advance was four, and four participants didn't get to know the questions beforehand, so 50% of the participants knew the questions and 50% of the participants didn't know the questions before the interview.

5.1 Security incident management process

The questionnaire was divided into two different themes, and the first theme was security incident management process. The purpose of questions in this theme was to gather information about the knowledge of security incident management process in use, as well as gain feedback on what sections of that process are seen as insufficient and require some development.

These answers are then analyzed and used to create suggestions in steps that require development. Suggested development needs are also coming from possible identified problems in current security incident management process documentation.

Security incident management process that is currently in use can be simplified in order to show the route on how the process would go through in normal case. Full security incident management process would have some deviation in cases where the occurred security incident would be considered as significant, which then causes process to start possibly crisis management process or major incident management process. Simplified security incident management process is shown in Figure 3 below the listing of phases of security incident management process.

1. Identification, some impulse is received that is being responded by creating a ticket
2. Analyzing, first response studies the incident and determines if the incident can be solved in the first level or if it needs to be moved to another team.
3. Response, some actions are taken to resolve the incident.
4. Documentation, report the incident to ticket.
5. Closure, close the ticket
6. After actions, start the change management process if needed.

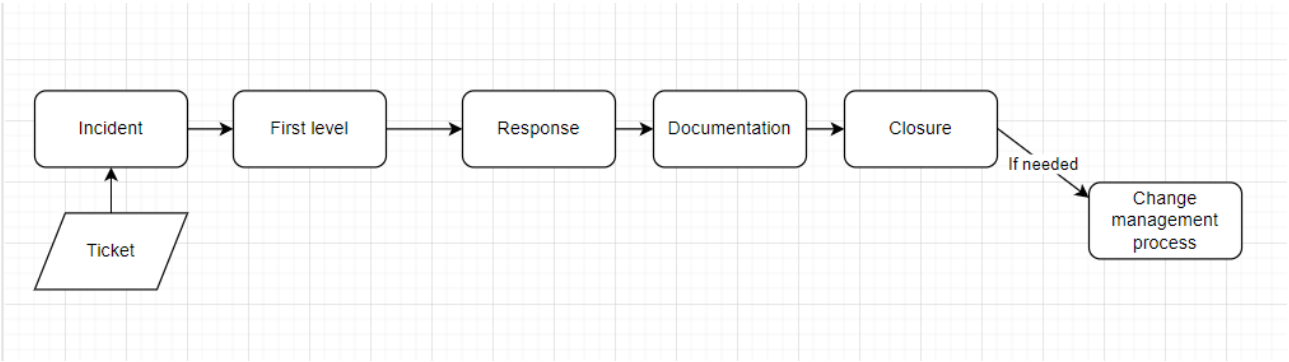

Figure 3 Simplified security incident management process

In current security incident management process first level handles the tickets when their impact is considered minor or false positive, on other cases the ticket is handled in technology teams with the help of assigned incident manager.

5.1.1 Awareness of process

The first question was there to determine how well organizations security incident management process is communicated to different teams, is the process in use well known between all the specialists that work within cyber security in one way or another or has the documentation just been created because it must exist, but it isn't being used efficiently.

The question that was used to determine all this was;

" Define different stages that are part of the current security incident management process."

The answers from participants varied widely in this particular question, the basic understanding of the security incident management process was there, but only the first response was answered by every participant. The variety of answers showed more that people are familiar with the subject on some level, but general knowledge about the documented security incident management process didn't seem to be communicated towards different teams that are working with security incidents.

5.1.2 Development needs

Second and third question that were included in the first part of the questionnaire were determined to gain information on development needs in the security incident management process from the specialists that are working within the field of cyber security in a way or another.

The questions that were used to gain this information were following;

> "Can you name 1-3 stages you think that should be developed more?
> Please could you tell why you chose these stages in more detail?"

On average participants named 2 stages that they thought should be developed. One participant didn't find any development needs in the process, this participant didn't have a clear picture on the security incident management process, so that might be the real reason why no development needs were identified by that participant. Second participant that brought only one development need up, identified a need to move away from 2 different management platforms and use only one as this would probably enhance the workflow as there would be only one system to have everything on it and specialists wouldn't have to work between two different systems.

62,5% of the participants noted that identifying the security incidents should be developed more, 25% of the participants thought that this should be done by automating at least some parts of the incident identification. Post incident was given as a need for development by 50% of the participants, the need for this was improving the documentation level of the occurred incidents in tickets. Other take on this need for developing the post incident phase, was to answer the need for following up on the incidents, improving the knowledge on what happened and if the incident could have been managed better. Development needs that were given by the participants can be seen in Table 1 and percentages of development needs by participants can be seen in Table 2.

Table 1 Development needs by participants

P1	P2	P3	P4	P5	P6	P7	P8
No development needs	Identification	Identification	Planning and preparing	Processing	Identification	Analyzing	Post incident
	Post incident	Processing	Identification		Post incident	Post incident	Identification
			Communication				

Table 2 Development need percentages by participants

Identification	62,5
Post incident	50
Processing	25
Analyzing	12,5
Planning and preparing	12,5
Communication	12,5

Other development needs that participants identified in incident processing, communication and analyzing the incidents. On processing the incidents the main need to clarify on what to do once the incident has been processed, analyses have been made that there is a possible incident, but no plans are made on how to resolve those as the ticket then just gets moved to next team and hope that the incident gets solved as there is no follow up. Development needs in analyzing were actually the same as the development needs identified in processing, taking the proper actions after the incident has been identified and analyzed are sometimes lacking.

Finally, need for developing the communication was identified as well, this could be developed by adding more transparency between the teams and incident handling and management. Often times different technology teams aren’t talking enough, and after incident has been handled, the information then doesn’t move between the teams and the information is kept within the persons that were working with the incident. One part that could also improve this was in close relation towards the planning and preparing phase, as there should be persons with mandate to gather a team with skills needed on resolving incidents when they occur.

5.2 Security incident response team

Second theme in the questionnaire was about security incident response team, the purpose of this section was to find out general knowledge on what the security incident response team is, how does it add value to the organization and what are the skills that are valued in a such team. Valued skills were not necessarily technical skills, as the question was aimed for more wide area of skills.

Answers gathered from the interviews are then analyzed to create a recommendation on organizing virtual team, what kind of people it should contain and what are their capabilities to handle security incidents.

5.2.1 Awareness on what Security Incident Response Team (SIRT) is?

The first two questions were there to gain understanding on how well participants knew what kind of tasks SIRT might be doing and how do they add value to the organization. As the role of SIRT can vary widely between organizations based on their needs, there is not a universally correct answer to what SIRT is, this question was there more to gain understanding on awareness on general level of understanding on SIRT.

The questions that were used to gain this knowledge were;

> *"How would you define what Security Incident Response Team (SIRT) is?*
> Which needs could be addressed by having a Security Incident response team?"

Answers gained for the first question varied a lot, some participants kept it short and simple where as others gave very specific answers on what they believe SIRT would be doing. Participants were given a short and simple definition of SIRT by the interviewer after they had answered first, the definition that interviewer gave was;

> *"Security incident response team is a team that handles identified security incidents"*

Answers for the second question kept the same line as answers to previous question, there was a variation mostly in length, but the overall knowledge on why SIRT would be formed, and which needs it would answer was on a very good level. Answers also varied depending on participant's

answer to the first question, so this would also be giving a bit more details what role they believed SIRT would fill.

5.2.2 Determining on what skills are valued for SIRT

Third and final question that was included in the second part of the questionnaire was determined to gain information on what kind of technical or non-technical skills, the participants saw as an important set of skills or requirements for successful SIRT.

Final question that was used to find these skills was;

> *"What skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?"*

Participants gave a wide variety of skills, but they all mentioned that technical skills are needed in one way or another, it doesn't have to be a requirement for everyone in SIRT to have those technical skills, as some tasks could be delegated to teams that main focus is on specific technologies, e.g. Windows knowledge.

Results are grouped roughly in the following tables for easier presentation of answers, first in Table 3we can see answers given by participants, and in the Table 4 we can see percentages on skills that were repeated by participants, technology knowledge was grouped from multiple skills, those skills contain following skills that were mentioned;

- Windows;
- Linux;
- Mac; and
- Security products;

Table 3 Skills given by participants

P1	P2	P3	P4	P5	P6	P7	P8
Technology knowledge	Calm / Patient	Technology knowledge	Technology knowledge	Red team knowledge	Calm / Patient	Communication	General cybersecurity
Cybersecurity experience	Management	Understanding logs	Mandate to act	Self-developig	Systematic / Analytic	Group activity	Technology knowledge
Network knowledge	Delegation	Communication	Management	Calm / Patient	Persistence	Technology knowledge	Organizational knowledge
Self-developing	Documentation	Delegation	Business knowledge	Communication	Technology knowledge	Mandate to act	Delegation
Passionate	Communication	Documentation		Documentation	General ICT		
Precise		Organizational knowledge		Overall experience	Legal knowledge		
Calm /Patient							

Table 4 Percentages of repeated skills

Technical		Non-Technical	
Technology knowledge	75 %	Communication	50 %
Network / ICT	25 %	Calm / Patient	50 %
Cybersecurity	25 %	Documentation	38 %
Red team knowledge	13 %	Delegation	38 %
Understanding logs	13 %	Management	25 %
		Organizaztional knowledge	25 %

As we can see from the results, non-technical skills were highly valued, and those skills were given more often than the technical skills. Good communication and documentation skills were valued, as well as ability to stay calm and patient during possibly stressful security incidents. Communication and documentation skills were mentioned often and had different views on why they were thought to be so important. Communication skills were thought to be necessary because in larger scale incidents there must be some communication towards customers and possibly different authorities. Documentation was important, as that could be beneficial in lowering the reoccurring incidents, as well as it would transfer some knowledge between team members, or employees in general.

Organizational knowledge was valued as it was seen to shorten the time it takes to find suitable persons to take part of resolving the incident. Mandate to act was mentioned by couple of different participants, as this was seen critical thing to be established and determined prior to any incidents. There should be personnel with the mandate to act when security incidents occur, and team must be gathered to resolve the incident. General management and leading skills were also mentioned.

Business knowledge would be beneficial to assess the incident's criticality in some cases. Legal knowledge was also mentioned, as some incidents might require actions regarding data protection regulations or communication with authorities.

As some technical skills that were deviating from the general answers were red team knowledge and ability to understand logs, both very good skills to have in SIRT. Red team knowledge adds different perspective to identifying possible vulnerabilities or preventing malicious actors to perform

actions they are after. Log reading skills was seen as beneficial skill, as raw logs themselves don't provide too much information to first response team. Some warning level logs, might not actually mean anything, or shouldn't even be categorized as a warning. Ability to understand logs gives ability to develop systems to give less false positives and therefore it would lower the number of alarms, tickets and required actions.

Overall experience in the ICT field, no matter if was purely from the field of cybersecurity was seen as beneficial as well. This would allow team to have people with wide area of knowledge and experience from different incidents or happenings, which then would result in better handling of situations as some of the situations could have been gone through beforehand by someone in team.

6 Conclusions

Maintaining and continuously developing security incident management requires regular reviewing the documentation, getting feedback from the personnel that are working with the processes and making sure that the process is known to people who should be working according to these processes. Base for security incident management process is often similar no matter where the process is being used, but they can vary based on the needs of the organization where the process is going to be used.

6.1 Results for security incident management process

Based on the reviewing the current state of documentation and data that was gained through conducting a structured interview with personnel who are working with security incident management process in one way or another, the biggest need for development is documentation and communicating that documentation to the personnel who are expected to work according to the process.

Documentation should be kept as simple as possible, so the process is easy to follow and understand, at least the general level of this documentation. Whereabouts of the documentation should also be communicated to the personnel and possible misleading documents should be moved into place where it shouldn't come up and possibly mislead someone who is trying to look up the process. There can be additional documentations that are going deeper into the process, but this could be designated towards the people that are going to need it.

The process should be transparent in a way that everyone who needs to read it can get the picture on what to do, who are the ones doing actions and how could they contact someone who is responsible for the process management.

Interviews showed that biggest need for improvement is identifying the incidents, even before they occur, so there should be some automation implemented that would gather data for possible vulnerabilities, before they are exploited, and actions could be taken in preventive manner.

Post incident was the second thing that came up in 50% of the interviews. These answers indicated that post incident should be improved, this phase was often overlooked or not done at all. This means that one of the most impacting phases for improving security incident management process has been neglected and development is not happening properly. Post incident should be gone through after every incident by the experts that were part of the team that was resolving the issue, as well as the incident manager that was guiding this team during the incident. Conducting these events after every incident and documenting the incidents properly would greatly improve security incident management process in the long run, as well as help prevent similar incidents in other customer environments in the future.

Processing was seen as a problem for couple of participants of the interview, but this problem could be solved with proper documentation and guidance in the first place. So, focusing on the simplifying the process and making it so that it is easy to understand what to do for the people who are expected to do something for the process could help removing this development need in the future.

Planning and preparing also needs some improvement so that the process would go smooth, and incidents could be resolved as soon as possible. Making sure that the process focuses on resolving the problem, and only resolving the problem during the incidents is the main priority, would result in less time wasted in other not necessary tasks for resolving the incident. After the incident has been resolved and after-action report created, then there is a time to think if there are some possible services or products that could be offered to the customer, either internal or external. This phase also answers to those needs in documentation, communication and identifying the incidents.

Finally, there should be regular training for the personnel that are working with these security incidents where the process would be gone through either in theoretical level or in practical training, possible development needs could be identified, and overall practicality of the security incident management process could be tested. This way the process could live as a healthy process that is being improved regularly and people that are part of working with the process would be familiar with it.

6.2 Results for security incident response team benefits

Benefits of working with virtual SIRT are that mainly the core of this team can be focused to managers, communication people and legal personnel who are not necessarily required to have deep knowledge on cyber security. Even the personnel who focuses on communication or legal can be optional, as they can be called in during the incidents that require their expertise. This means that all the technical, legal and communicative personnel can focus on different tasks during the normal operations in organization and gather as a team when their expertise is needed during a security incident. For technical personnel this would also mean that they should have more time to gain more expertise in different areas, study new threats and vulnerabilities, develop different systems that can improve the situational awareness.

These specials should be considered as extra for those technical teams, during the time of normal operation, as they are required to drop down their tasks if a security incident occurs. This means that these specialists can't really have sole responsibilities in time critical customer projects, because it is impossible to predict how often and what kind of security incidents are going to occur.

As the organization is already working in some ways with virtual SIRT, there would be not so many changes required for it to be working properly. Main focus would be communicating this better with the team leaders, naming the incident managers that have the mandate to call in participants for working with occurred security incidents and have some personnel identified beforehand that would be needed to join in security incident response team if their expertise is needed to resolve incident at hand.

The core of this virtual SIRT should consist of people who have the ability to manage and lead during the security incident, as well as have the mandate to call in needed resources from the different technology teams. People in the core should also have knowledge of the organization, so they know where those needed resources for each incident case could be allocated. Legal knowledge should also be present, as well as communication skills and knowledge on who to contact and what kind of informative steps should be taken along the way of different incidents. Documentation of the incident should be thorough, and this is something that should be made sure during the lessons learned phase, so there shouldn't be any more tickets of incidents with description of "this is fixed".

7 Reflections

This section goes through the reflections and thoughts of this thesis process, considers ethics of this work, how the process went overall and what kind of future research there still might be regarding this topic.

During the research I noticed that majority of the published papers and research were based on ISO 27000-series, NIST CS800-series or ITIL framework. This showed in a way that researches showed very much similarities between those, as the base of that research was the same. Biggest difference between those papers were usually the field they were applied to, even when the base is same, there are always some differences depending on the applied use case, as not all organizations are the same and this subject cannot be generalized on detail level.

7.1 Ethics

During the literation phase of the interviews I had to think the ethics of this research, as personnel had to be anonymized and some details had to be censored as well as the language had to be translated from Finnish to English. Literation had to be done in a way that participants couldn't be easily identified and no sensitive data should be left away from the interviews that are then part of this thesis, and at the same time the context of the interview should still remain the same, so those appendices could be used by someone else if they wish to conduct additional research or review the validity of the results that I have presented in this work.

7.2 Thesis process

Doing the literature review was probably the most rewarding and frustrating phase of this thesis, there was quite a lot of literature for this subject, but as they mostly relied to those three biggest standards or frameworks, they often showed quite a lot of similarities.

In the beginning phases of this thesis work I tried to find possible research subjects from previous work but noticed that they often noted in their possible future research section that the subject would be interesting to further research on how it would work in some other field, so that didn't really help with finding some suitable research questions.

One problem that I felt like having during this research process was that when I was having conversations with people who were working with cyber security, they wanted to help, but at the same time they felt like they couldn't really tell me anything, due to the nature of security incidents. This was then tried to avoid in a manner to conduct questionnaire where I wouldn't ask for specific cases or tickets, whereas I would focus more on general level to seek those problems that lied inside the current security incident process.

7.3 Possible future research

Due to the fact that this work turned more theoretical and suggestive results, it would be interesting to actually implement these steps into the real security incident management process and then gather data on how the incident management would improve. Problem with that of course is that no organization is the same, and this causes the problem that these findings cannot be implement straight into another organization's incident management process. However, these main topics can be revisited in another organization and see if there are any room for improvement, or if the process has thought about those steps and actions within those steps that this thesis suggests.

References

Aguilar, J., Abraham, B., & Moreno, G. (2009). *A security incidents management for a CERT based on Swarm Intelligence.* WSEAS Transactions on Computers, 2009, 8.8: 1398-1407.

Aleksandrova, S. V., Vasiliev, V. A., & Aleksandrov, M. N. (2020). Problems of Implementing Information Security Management Systems. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 78–81. https://doi.org/10.1109/ITQMIS51053.2020.9322896

Berger, D., Shashidhar, N., & Varol, C. (2020). Using ITIL 4 in Security Management. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS49300.2020.9116257

Boks, J. (2022, February 24). *What is swarming? And how does it benefit your IT support?* TOPdesk Blog. Accessed on 14 May 2023. Retrieved from https:/blog.topdesk.com/en/itsm/what-is-swarming/

Clark Matt, S. (2023, March 23). *A guided tour of the 2023 Threat Detection Report. Red Canary. Accessed on 26 April 2023. Retrieved from https://redcanary.com/blog/2023-threat-detection-report/*

Consortium for Service Innovation. (2018, March 29). *Intelligent Swarming. Consortium for Service Innovation.* Accessed on 14 May 2023. Retrieved from https://library.serviceinnovation.org/Intelligent_Swarming

Cullen, D. (2019). *Building a Computer Security Incident Response Team: Required Skills and Characteristics - ProQuest. https://www.proquest.com/openview/55eca07db594fabf9039a2ad6c9bea9d/*

Darren Death. (2017). Information Security Handbook: Implement Information Security Effectively As Per Your Organization's Needs. Packt Publishing.

de Jesus Martins, R., Knob, L. A. D., Silva, E. G. da, Wickboldt, J. A., Schaeffer-Filho, A., & Granville, L. Z. (2019). *Specialized CSIRT for Incident Response Management in Smart Grids.* Journal of Network and Systems Management, 27(1), Article 1. https://doi.org/10.1007/s10922-018-9458-z

Dsouza, Z. (2018). *Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?* Federal Communications Law Journal, 69(3), 201.

Haapakoski, M. (2018). *Incident management in multi-vendor environment.* Cyber Security. https://urn.fi/URN:NBN:fi:amk-2018061113471

International Organization for Standardization. (2022). *ISO/IEC 27001:2022*. ISO. https://www.iso.org/standard/82875.html

International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023*. ISO. https://www.iso.org/standard/78973.html

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885240

Jones, O., Gold, J., & Claxton, J. (2022). An exposition of the constructive research approach: A tactical treatise for addressing methodological and practical issues in organisational research. International Journal of Organizational Analysis. https://doi.org/10.1108/IJOA-03-2022-3212

Leanne, S. (2021, July). *Swarm intelligence: How human ingenuity is driving cyber threat actor evolution.* Accessed on 14 May 2023. Retrieved from https://www.linkedin.com/pulse/swarm-intelligence-how-human-ingenuity-driving-cyber-threat-leanne

Line, M. B., & Albrechtsen, E. (2016). *Examining the suitability of industrial safety management approaches for information security incident management. Information and Computer Security*, *24*(1), 20–37. https://doi.org/10.1108/ICS-01-2015-0003

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2014). Information Security Incident Management: Planning for Failure. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, 47–61. https://doi.org/10.1109/IMF.2014.10

Manage Engine. (n.d.). ITIL incident management process: 8 steps with examples. Zoho Corp. Accessed on 1 May 2023. Retrieved from https://www.manageengine.com/products/service-desk/itil-incident-management/what-is-itil-incident-management.html

Oyegoke, A. (2011). The constructive research approach in project management research. International Journal of Managing Projects in Business, 4(4), 573–595. https://doi.org/10.1108/17538371111164029

Reed, T., Abbott, R. G., Anderson, B., Nauer, K., & Forsythe, C. (2014). Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams. https://doi.org/10.1177/1541931214581089

Rudzitis, R., & Dorogovs, P. (2018). Research and Management Security Incidents. 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 1–6. https://doi.org/10.1109/AIEEE.2018.8592159

Ruskojärvi, T. (2020). Cyber Security Incident Management Process in NOC/SOC Integration. https://urn.fi/URN:NBN:fi:amk-2020061218529

Villegas-Ch, W., Ortiz-Garces, I., & Sánchez-Viteri, S. (2021). Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. Computers, 10(8), 102. https://doi.org/10.3390/computers10080102

Appendices

Appendix 1. P1 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. So, we will start with the security incident management part and the first question is: Could you describe the different stages that are part of the current security incident management process.

P: So, umm, to name different stages, I don't really quite understand what we are after here with the security incident management as our team is only doing first response on incoming tickets. So could you maybe elaborate a bit more.

I: When an incident has been identified, what different stages there are for the incident management.

P: If we identify something is malicious or alerting, then we delegate it to another team that will handle the incident and that is it.

I: Okay, that is all right. Then the next question, can you name 1-3 stages you think that should be developed more.

P: There isn't really anything that would require any development as the tasks are so simple for us. If we find anything we will just move the ticket to another team with the information we have.

I: And that is working just fine?

P: So, there isn't really anything that would require any development.

I: So then there the final question about this theme would be that could you tell why you chose these stages in more detail, but as there wasn't any, we can skip this.

P: Yes, there really isn't anything to improve.

I: Yes, okay, then we will move on to security incident response team, and the first question is: How would you define what Security Incident Response Team (SIRT) is?

P: So, who are part of it or?

I: What does it do, what is role of the SIRT?

P: Their role is to continue the process of solving the incident and figure out if the incident is malicious or not and if it is malicious, they will continue on with forensic and try to find out if the incident has spread out more, and they will be in contact with the customer about how to deal with the situation, this is my view on this.

I: Yes.

P: We don’t really do this so, this is about general level of this, like I said they will continue with the investigation and if there is something then they will move on with forensics and mitigate actions are also part of this depending on the security incident.

I: Yes, okay. So, I have marked for myself that I will give a short description about the SIRT after the participant has given their answer. So, in all simplicity security incident response team is a team that handles identified security incidents. Just like you just told me.

P: Yes.

I: So, then the next question goes like this:

Which needs could be addressed by having a Security Incident response team? Why this team is formed? Or should be formed.

P: Because you need to handle those security incidents. That is it, pretty much nothing else to it.

I: Thank you. And finally last question: What skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: Different operating systems are needed to be familiar with, windows, Linux, mac. Those need to be familiar with.

Need to have experience especially on how the windows works, how different areas affect on different things in case of an incident.

Cyber security, at least basics should be known very well and even on more advanced level and would be preferred if would have been working with cyber security for a longer period of time already.

Network understanding should be at least on some level, like how the network is working, ip addresses which are internal and which are external and so on.

Person should be continuously self-developing, because there are new vulnerabilities daily and all the time that need to be followed and be on top of.

Like in our team we are reading about the new vulnerabilities every morning, it takes time, but is mandatory so we know what the new vulnerabilities are and how it affects.

I think that is about it, of course there would be a need to have a passion about the job and person should be precise and patient, I think that's it.

I: Good, thank you. Nothing else on this interview, now there is a free speech if there is anything you would like to bring up or anything else, preferably on the topic.

P: Nothing on this subject I can think of.

I: Okay, then I would like to thank you for taking the time and answering though this questionnaire.

P: You are welcome.

Appendix 2. P2 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. Both sections have 3 questions and after that is a free speech.

P: Ok, understood.

I: So, we will start with the security incident management part and the first question is: Could you describe the different stages that are part of the current security incident management process.

P: Do you want the answer more on general level, like if there would be a crisis going on or just a basic incident.

I: Basic incident

P: It starts with finding the incident, whether it came from the customer or internal employee or something like that, in the simplest form it comes with the ticket that includes that incident.

After that we go to first responder, first level that starts investigation and tries to figure out the level on this incident, if its minor, major, or what level of criticality the incident is.

After that according to the first responder's skill level, mitigation actions could be done if possible and skill level is sufficient for that.

If incident cannot be resolved here, then the incident is moved to second or third tier, or if this is identified as critical at this point, it should be thought if crisis management team needs to be assembled or separate SIRT team to investigate.

Based on that incident then is either tried to be solved or escalated more. Next level basically does the same, either it tries to resolve the incident or reassess the need for crisis management team.

If it goes to crisis management, then there are different processes for that, but we don’t need to go there in this?

I: No need to go there.

P: Then after or hopefully the incident has been resolved, then corrective actions are being made, then one part that doesn’t always come true, is the lessons learned which goes through why and how this happened.

This then shows that the incident couldn't have been prevented, or if it could have been prevented, then we could also prevent it to happen in other environments and take action to those. Then new tickets could be opened and resolve those.

Those then could start a new process that might require some planning or starting projects, scheduling and change management etc.

But maybe in short: Identify the incident, make the assessment of the criticality, make actions which includes the mitigation/repairing or escalation to the next level, on escalation level figure out if incident can be resolved or if there is a need for more drastic measures.

After the incident reviewing the incident and figuring out why this happened and what could be done better in the future.

I: Thank you, then the next question is if you could name 1-3 stages that you think should be developed more and if you can name more than you could you please put them in priority order.

P: Well, the correct identification of the incidents, that is something that should be developed, I mean that when incident arrives, it is then identified if the incident should be investigated and its not handled like that the incident is just 'resolved' back to green and forget about it.

It should be really identified if this is something that could reoccur, or could this have a larger impact that would cause other problems. So, the incident should be identified and properly classified.

Secondly, lessons learned side, once the incident has been handled the same should be done there, so that the fix wouldn't be a temporary fix, or patch the wound but leave the wound behind.

It should be thought how the fix could be done permanently and for real in that environment where the incident occurred.

Those are the things I would see that would require developed and in that order for priority as well.

I: Okay, thank you, could you tell me in more detail, even though you already gave a very good reasoning for those steps about why you think, but anything else to add?

P: I don't think that those things aren’t being thought enough when the incident occurs, no matter if its big or small incident, especially on the later stages of the resolved incident.

They want to close tickets and out of the mind just as fast as possible instead of thinking more thoroughly and going through more investigations if something larger should be done like changing platforms or something like that.

I: Okay, thank you, next we shall move to security incident response team theme. First question is how would you define what security incident response team is?

P: It is a team that reacts to incidents once they appear, but also does pre-emptive work and monitors the situation in the environments and tries to identify possible problems in advance, like operating systems that are about to expire in the near future.

They could identify those expiring operating systems or expiring software and fix those in advance before they become a problem. Managing vulnerabilities and once the incident has occurred, they work to resolve that incident and tries to do it without the need to escalate the incident to crisis management or so.

I: Thank you, and I have this very simple and general description about the security incident response team that I will tell participants once they have given their answers. So, in all simplicity security incident response team is a team that handles identified security incidents, of course could also be part of many other things, but yeah.

Next question is about which needs could be addressed by having a Security Incident response team?

P: In general I think if there would be a SIRT team, that would react to incidents and would also do that pre-emptive work but priorities on resolving ongoing incidents, like putting down fires.

Hopefully that wouldn't take all of their time, and then while they are not resolving any ongoing incidents, they would try to prevent security incidents from happening.

I: Thank you, and then the final question:

What skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: Well, both are needed, technical and non-technical personnel, of course it depends on where the SIRT is working, but it doesn't really need the know-it-all specialists, but people with experience from all around that have seen different things along the way and can use that knowledge to prevent panicking. So, if the situation looks bad, there wouldn't be too drastic measures made in hastily manner. Situation should be taken calmly, assess the situation and then do the necessary actions.

These guys of course need a leader who can lead the group in calm manner and tell what to do and when to do, leader doesn’t necessarily have to be technical, and if leader isn't really a technical person, then he has to know how to ask the right questions from the team and receive the information from the specialists and then proceed with the steps that are needed and what are the priorities.

Then this isn't really a requirement, but it would be really good if there would be a person who is really good to document things, keep a log on the incident, write things down.

I don't mean that what I have seen that there is a description of the problem, and it has been resolved with text "fixed", but that the ticket would have information on what was done and why those things were done.

Then it depends on where we are operating, but communication, whether it is communicating with the customer or internal people should be done properly, like if there is a bigger incident there should be some communication on what is going on to prevent panic.

I think group like that would already go pretty far.

I: Thank you, and then there is a free speech if you have anything to say about this topic.

P: No, not really about this topic

I: Then I would like to thank you for the time you took for this interview and wish you a good rest of the day.

Appendix 3. P3 Transcript

I: Interviewer

P: participant

I: I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. Both sections have 3 questions and after that is a free speech.

P: Alright

I: So, we will start with the security incident management part and the first question is: Could you describe the different stages that are part of the current security incident management process.

P: Well, as I am not really part of the management process other than reporting and as a technical person, but it starts with first response, some information comes from some source.

After that, the information that was received needs to be processed, before something is done with that processed information. Finally, some actions has to be done with that processed information.

So, in short; First the information is received, then the information is processed and finally actions has to be done regarding the processed information, then the process maybe shifts away from the incident. So, 3 stages.

I: Alright, thank you, then the next question is if you could name 1-3 stages you think that should be developed more?

P: Is this question about the current situation or in general?

I: current situation.

P: Automation for the first responding should be developed, now there is a lot of data that has to be processed which is raw and sometimes confusing,

the information contains a lot of human interaction which means that the information has to be brought up personally and manually in weekly meetings before anything can be done.

It would be better if these things would come up automatically. This is also probably the hardest thing to develop.

Second thing that should be developed is that what is done with that processed information, there often isn't a real plan on what to do with that information that was gathered and processed.

Often the information comes in a way that there is a vulnerability but no real plan what to do with that information. Process should contain a plan what to do after the information has been processed.

Not like just to give this information to expert and hope he does the right thing with it.

I: Okay, thank you, could you tell me in more detail, even though you already gave a very good reasoning for those steps about why you think, but anything else to add?

P: Processing the information works all right, the data is being processed and moved forward, but the thing is that currently there isn't so much data, so this works fine as it is for now, but if the initial data gathering would be automatic

then this processing data could also be in problem. Processing could be stuck in the middle because the information would come automatically there and not from human sources only. So maybe that wouldn't really work out either if there would be bigger amount of data.

I: Alright, that is all good, and next we could move towards the second part, which is about the security incident response team. First question would be: How would you define what Security Incident Response Team (SIRT) is?

P: Security incident response team is a group of people who gets information from different sources, both automatic and manual, which then processes the data and does something with that processed data, is the first responder of the incident.

Once the initial assessment has been done, then moves the incident to another group that handles the incident, because once the ticket has been made, doesn’t really belong to SIRT team, because it goes to post-incident.

I think that is a good line to draw for this team, SIRT is the first responder because it takes a lot of time to follow up on things and sorting out things.

So, I don't think that belongs to the SIRT team because there is a lot coming in and it requires a lot of staff, so I think post incident should belong to either manager that handles them forward or to completely another team.

Otherwise SIRT will be in a jammed state of there needs to be additional personnel coming in indefinitely.

I: Thank you, and I have this very simple and general description about the security incident response team that I will tell participants once they have given their answers.

So, in all simplicity security incident response team is a team that handles identified security incidents, of course that handling can be on whatever scale is determined, it depends on specifications on what is wanted.

So, moving on to the next question, and next question is about which needs could be addressed by having a Security Incident response team?

P: Is this more of a generic model, just so it’s not for our organization?

I: Yes.

P: Team is required once the organization grows, as small organizations might not really need it as there is a small amount of infrastructure.

Usually, the need for SIRT comes up after there has been an incident and you would like to fix those problems that came up during the incident, or you would like to be prepared for an incident in case one would come up.

SIRT also gives good feedback on what happens once there is a identified incident that requires actions, it would be better if you could reduce the amount of actions that are needed to be performed, which would mean you area actually in safer spot.

As it would be preferred state that if incident occurs, it would be handled automatically in most cases and the required actions would be more like a following it up on what happened.

If the team gets and task that required actions, it would mean that the security needs to be developed more, because then it again is a incident, and that is something that you don't really want.

So, in short, it answers to how fast organization is to react and resolve incidents.

For example, if you have no SIRT and there is a incident, what happens? Probably noting, but if you have a team, the reaction and resolving of the incident comes faster as it is standard thing to do for that team and you also can improve your security according to those findings from the occurred incidents.

So even if it might feel like a niece thing to have, it is pretty much required after organization grows big enough, as it frees up some time for people to focus on their own tasks.

I: Yes

P: So then for example Chief information security officer (CISO) doesn't have to do all of those tasks alone, following up on vulnerabilities and resolving incidents, because that is not really a core task for CISO.

I: Yes, that's about it. Then final question would be what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: Technical skills that would be required is absolutely ability to read logs, logs are dumb, especially if they are misconfigured and for example if there is a warning level log, it might not actually be a real warning that requires actions.

So, logs require filtering in order for them to be truly useful and this also means that you could then improve the logging capabilities and systems to get better and more accurate information.

For example, if you receive an alert from logs and you see that it's not really anything important, you need to be capable of fixing that faulty log as soon as possible. This would then reduce workload in the future, I think that is the most important technical skill.

For non-technical skill it would be that how you are able to communicate tasks that require some actions from someone else, it requires a lot of knowledge on that possible incident, on what it might actually impact.

You would need a lot of knowledge about the organization, people who are working there, and you need some knowledge on how to write a proper report. It's one of those soft skills that is required to know.

Like how you can give that most important piece of information to others in the most simple way that it gets understood.

I think those are the two biggest skills that are required.

Of course, if you work with windows, you need to know your way around windows and if you work with Linux you need to know your Linux, so maybe I wouldn't really put a person to incident team if they don't have experience on the technologies that are currently in use.

But those two skills are something that aren't really being tied to any specific technologies.

I: Yes, very good skills that you mentioned, now there is a free speech if there is anything to say about this topic.

P: Good questions, umm, I don't really have any additional questions in mind.

I: Alright, then I would like to thank you about your time and answers. Have a good rest of the day.

Appendix 4. P4 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. Both sections have 3 questions and after that is a free speech. So, let's start with that first question from security incident management process, which is: Could you describe the different stages that are part of the current security incident management process?

P: Well, it depends on how the incident starts, but initiation could come from normal customer service work where incident could escalate into security incident from different inputs, so perception phase.

Second way is that alarm comes from automatic services, which then indicates that it is a high probability that it is security incident from the beginning, or the initiation could come through different customer channels.

First phase for the security incident process is classification, which creates analysis on which actor this case would belong to and would continue handling the ticket.

Second phase then comes after the security incident has been identified, then the incident should be transferred ticket into the que for the team that manages security incidents, now depending on the incident on what type of security incident has been identified, it gets transferred into team that will start handling the ticket, this is basically a first round of analysis for the incident.

After some kind of risk analysis has been done for the ticket, then the next phase can begin, and if we would go on with a normal case that there are already standard actions for resolving the ticket, then the mitigation steps could begin.

This means that there are some standard actions readily available for those kind of cases in the technology team that will be resolving that ticket.

Next phase is analyzing the case, how did the mitigation affected on this case and then closing the ticket, and when closing the ticket should be categorized if it possible in the ticketing system that the ticket is solved.

Now if we would go into the case where risk level is high enough and security incident is more serious than in that normal case, then we would go towards the process where we would call in our virtual security team, according to the needs of the case that is happening.

Then handling begins with the group analysis in order to understand what really is going on and where this affects. This then continues to estimate whether this incident requires inclusion of crisis management team or not, if this is a major incident of some kind, or if this is a more of an incident that is more of a specific technology incident that could be resolved in that way.

In this process, after the analysis has been done, it could also include other groups, like privacy, if analysis shows that it would be necessary. This also could mean that notification towards authoritative should be considered if it needed or not.

Customer notification also should be thought out, just like in smaller cases, but in these more serious cases, it might require a larger scale communication towards customers. This also could kick off different control processes and communication processes along the way.

This usually results in a forming a virtual team that continues with solving on those more serious security incidents. It is a hard to say beforehand, on what are the needs for that team in each case that are required to join on that virtual team.

This is basically on what is going on, I understand that if we go into more literature and theoretical path it might be a more finely divided.

I: Alright, good, thank you. Now the next question is if you could name 3, or 1-3 stages you think that should be developed more? What kind of stages should be developed and if you can name multiple, then could you put them in order of priority?

P: I would like that give a few in random order and then I'll try to prioritize those.

So, regarding the security incidents, the overall documentation, how we are managing data and how we are managing configurations, that is probably the most important as well, so that we are up to date all the time on the view of vulnerabilities and services we are currently providing, so we would know which services we should worry and know the state of security they are in.

That would be the supporting process that I would like to develop in a major way.

Other thing that would be important is automation, we don't really have a proper components in place, which of course would need the configuration management before they would give anything useful to us, but from the incident process perspective, we could then generate automatically analysis on the incidents which then would give a better view and understanding to the incident manager.

This would then improve the time it takes to identify the impact of an occurred incident and what services and customers it is affecting. So, this could also maybe give ability to create tasks before any incidents even would occur.

But also, we could also automatically identify possible risks and that would be more easily transparent to different technical asset owners, from small servers to bigger services. This would improve the time it takes to act during incidents and have more up to date information.

Now there is that need to unify different areas and services regarding the way of managing incidents, now it feels like we are working inside our own silos, which then causes problems on identifying who is responsible for each service outside those silos or teams.

This then causes some delays during an incident because it's hard to know on who is responsible for some services and it takes time to figure out who is needed to give assistance during an incident. Also, the problem if the incident is resolved inside the silo, then there isn't any transparency on what was done and what happened.

Mandate should be given beforehand, and it should be clear to all those different teams, so in case of an incident it would be clear to everyone what tasks can be given to who.

Also, something that affects to all those 3 is risk management, and even while we are trying to identify risks all across the services, identified risks usually happen to stay only inside the specific technical teams or service teams and the transparency doesn’t happen.

I: Good points there, now the next question would be if you could tell me in more detail, even though you already gave a very good reasoning for those steps about why you think, but anything else to add?

P: Yeah, well that managing risks and dependencies should be identified better and like we have different frameworks for cyber security, like ISO 27001, which is one valid argument.

We have to be able to show that we are working according to the requirements that framework is setting, just like we are, but we would also like to be better with constant development in this subject.

Which is one of the requirements in ISO frameworks, that we have to be able to further improve our processes.

I: Alright, thank you, next we can move to that security incident response team. The first question is if you could tell me what is a security incident response team?

P: We don't really have a specific security incident response team, but we have something similar, which we are calling a cyber security virtual team, where the elements are similar to security incident response team but works more in a preventive way in a weekly spacing.

When called in the composition varies and can be very different each time it is called in, but there are people representing different technologies and production areas who then can gather the specialists when they are needed.

So, the basic response if more like in a daily production, so this model relies in that the services we are providing, we are also using those same services ourselves. This is the basic foundation for this.

I: But if we are thinking about more general level, what is a security incident response team?

P: SIRT is a team which is gathered once there is a need or security incident has been identified.

I: Alright, thank you.

P: And SIRT actors are there depending on the organization.

I: Ok, yes, so I have been giving participants a so-called textbook definition of a SIRT after they've given me their answers, so security incident response team is a team that handles identified security incidents, not going into too deep on what it actually includes.

P: Yes, that's like it can very much vary depending on what the organization is providing and how the organization thinks what is that they think is relevant.

I: Yes, then the next question would be like which needs could be addressed by having a Security Incident response team?

P: Well, it is a fast response team, so they answer into acute security incidents or incidents that could be classified as such, of course they are doing analyzing the incident every time if the incident even a cyber security incident was or not.

But yeah, every incident is handled in a way that the incident handling is required. First with smaller team and then if needed in a larger team, then the sense of urgency could be gained into the need of resolving the incident.

I: Yeah, then the final question of this SIRT section is what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: Well yeah, about the skills, I don't want to go too deep into competence level on the technical side, because they are obviously needed anyway.

But skills that are needed, there needs to be a person that has the mandate to call in security incident response team and manages their doings and has to understand the role of SIRT and role of the person who is managing and calling in that SIRT, doesn't matter if this is information security manager or some administrator on some business area or a technical lead.

But property that is needed is the ability to start handling the case in a hastily manner, analyzing on who has to be involved and being able to lead this incident, typically a part of management, leader of a team, which isn't really a requirement but has to have the ability to lead the incident.

Skills that are needed are very much like major incident manager has, so has to have ability to take leading role during the incident and this person has the mandate and understands that the mandate has been given and it can be used.

So, some kind of bravery to act as a leader instead of just a employee who is just doing what is being told.

I: Alright, anything else or?

P: Then if we look at the competences, a good incident leader, if we would have the luxury to select the leader according to their competences, then of course it would be great if we could allocate someone who is an expert in the field of server or virtualization platforms to lead the work.

That could also be a challenging because, it could go too deep into the technology, but some level of knowledge would be beneficial, so they would understand some dependencies on different technologies and services what affects what.

Also one part is that basic business understanding, so there would be understanding on what dependencies are between promises made to customers, customer needs and regarding the compliance, like what kind of customer base is being affected, like if it is public administration, or personal information or if the incident is again some smaller kiosk, like florists, there are very different urgencies regarding the customer base who it is affecting and what kind of team should be gathered.

I: Very good answers, that’s about it with the questions, now there is a free speech if you have something in mind regarding this topic.

P: Well maybe just like the world isn't ready yet, so security incident would require additional development, and that development should begin from building up understanding in process areas and documentation should be updated.

Also, it wouldn't be a bad idea to have these role actors in different areas for that SIRT like actions, so now if there is a maybe behind the curtains virtual team movement, why it couldn't be more like a public thing, so different parts of organization should include more of those security incident lead kind of roles, that would include different technology areas.

Then we would be able to gain resources more easily during the incidents and this wouldn't be such a big surprise to those persons that they could be called in. This maybe should be developed in the future.

I: Thank you very much for taking the time to participate this interview.

P: Thank you for creating such a nice interview, and I hope that you got something out of this interview.

I: Yes, I sure did, thank you and have a good rest of the day.

Appendix 5. P5 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. Both sections have 3 questions and after that is a free speech. So, the first question is Could you describe the different stages that are part of the current security incident management process.

P: Identifying the problem, creation of ticket.

Then the ticket is moved to handling team and it should be done in a window of service level agreement and it should be resolved as well inside those time windows that are agreed on the service level.

Communication to the affected parties, like if there is a system outage, so people know that there isn't a need to create another ticket about this situation because it is already being worked on.

Then the outcome of the solution from that incident management, if incident has been fixed with a work around, then the root cause needs to be identified as well.

Always the root cause should be identified so the same incident wouldn't occur again as there could be suitable alarms created that would show in the future if there would be signs that same is happening again.

Once everything has been taken care of, then reviewing the ticket that everything is in order and then it can be closed.

I: Good, thank you, now the next question would be on could you name from 1-3 stages that you think should be developed more? Also, if you can name multiple, then it would be great if you could put them in order of importance.

P: Currently I think the most important thing is to be able to move the process into the new service platform from the old one and start using only the new one. The ramp down is ongoing, but it should be finished.

That's pretty much what I can come up with.

I: That is okay, then the third question would be if you could tell me a little bit more detail why is that?

P: Because I think that old system is being removed, and I am not quite sure on how the workload is divided between the new and the old system, but I think it can be quite a difficult if you have to manage tickets in two different systems.

I: Okay, thank you, good answers. Then we can move on to the security incident response team part of the interview, and the first question is what is security incident response team?

P: I can't really recall hearing a team named kind of like that, but based on the common experience I would say it is first responder, a team that is receiving the tickets and investigates the situation and resolves the ticket if it can be done in a hasty manner.

If the ticket cannot be resolved fast, then it should be moved to the next level who will take care of the incidents where resolving those incidents could take a bit more time.

I: Alright, I have been giving participants a so-called textbook definition of a SIRT after they've given me their answers, so security incident response team is a team that handles identified security incidents.

P: Okay, that is well compressed.

I: Of course, it doesn't give a very detailed definition on what SIRT could hold in, because it is more of the organizations to define what they want it to do and perform. The next question would be that what are the needs that SIRT answers to?

P: Hmm, I have to think a bit more for this, are you after technical or business kind of needs or a bit of both?

I: Maybe a bit of both, like why would anyone want to create a team like SIRT? What is its function inside the organization?

P: Okay, so the function of the team like this is to protect organizations IT environment and the business need is maybe the most important, even though team like this isn't really producing any sales per se, it can manage larger risks and avoid things like case Vastaamo which would then result in a business going down at once.

Then if we are talking about SIRT that is selling this as a service to customers, then the risk management is still there, but it also generates sales for the organization.

I: Good, thank you. Then the third question about this subject is what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: There is a need to understand both, technical and non-technical things. The team dynamics allow that one person could be more technical and other could understand more of those processes, because overall it is the team that is doing things.

One should be able to see things from the attacker point of view, like what would I do if I was a hacker and wanted to gain access to some place and cause havoc.

From having the ability to do so, it could allow you to prevent hackers to perform actions they are after.

There is also a need to be able to stay up to date on different vulnerabilities, threats and what malicious methods are trending right now.

Then of course there is a need to be very patient, ability to withstand pressure and haste, because these things can sometimes be very demanding situations and one should be able to stay calm.

Also in more demanding situation, organization should be able to get organized in a way that someone would take care of the communications and the technical persons can stay focused on the technical side of things.

Then documentation skills are very important, in the most simples form the documentation is just writing things down to a ticket. Even if some key personnel would be unable to attend for any reason, like they are getting sick or not longed working within the company, the people who are still working would be able to perform.

People have a lot of know-how, the silent skills which then should be documented on tickets, this is just a one way to transfer that know how to other persons if something happens to the first person who was working with the task.

But yeah, quite a large amount of skills are needed, and being a part of SIRT isn't really a place to be for a beginner.

I: Alright, thank you very much, and now there is a free speech, preferably about this topic.

P: Yes, this was very interesting, and the time went quite fast, good questions.

If you think what happened to Vastaamo or Lemonsoft, where they actually informed publicly on their website and something in the media.

But these kinds of things can happen to anyone, so there is a need to be open when things happen, especially inside your own organization.

Like if some malicious actor gets in, I think the Lemonsoft handled very classy their situation and I would say that as there are these two very different cases, which kind of way of communication I would more trust, it would be Lemonsoft way, no doubt about it.

One shouldn't really be so ashamed of the incidents that have occurred because it could happen to anyone, but one should think on how to resolve that incident, how it should be communicated, should the actions be taken immediately or should it be investigated more.

I: That's right.

P: Second thing I would like to say, not only about the security incident response, but the cyber security of the whole organization the level of knowledge should be improved all the time, with all those small trainings, awareness programs and like those.

But the subject is very strongly that the user itself is the weakest link, no matter how much there is automagical defense mechanics, malware identifications, monitoring mechanisms, but the most significant risks are coming from the users.

I: That is correct.

P: But yeah, overall, this subject is one of those that there is a lot of work to do into the future and an employment can be rather safe if one doesn't completely screw something up.

I: But thank you very much for participating this interview and have a nice rest of the day.

P: Thank you.

Appendix 6. P6 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section. Both sections have 3 questions and after that is a free speech if there is time left for that.

I: We can start right away from the security incident management questions, and the first question is could you describe the different stages that are part of the current security incident management process?

P: Process includes identifying the incident, and during the identification phase, it is important to delimit which services the incident is affecting. So, the incident can be resolved as efficiently as possible.

After the incident has been identified, then the process aims to restore services back to normal.

Finally, it should be identified what caused the incident, and this should be documented as well for the future steps, like preventing similar incidents in the future.

I: Alright, then next question is can you name 1-3 stages you think that should be developed more, and if there are multiple, can you put them in order of priority?

P: Identifying and delimiting is important, so the mitigation and resolve incidents can begin faster.

Then identifying the root cause, and the documentation of those root causes for the follow-up measures is also very important.

From these two, in the long run identifying the root causes is more important.

I: Ok, now the third question is could you tell me why you chose these to require further development in more detail?

P: Reasoning could be that those steps allow to enhance the security incident management process, which leads to faster resolving of incidents and possibly lower the incidents caused by the same cause.

I: Very good answers, next we can move on to security incident response team part of this interview. Next question is how would you define what security incident response team is?

P: SIRT is a group of people within an organization, could also be group of external people in some cases.

This group is available when security incident has been identified, there are different roles within this team depending on their expertise.

For example, depending on the level of the security incident, there could be a need for leader, or there might be a need for communication or forensics, or some other areas of expertise.

I: Well said, now I have been giving participants a so-called textbook definition of a SIRT after they've given me their answers, so security incident response team is a team that handles identified security incidents. Of course, this doesn’t go too deep on what the team is actually doing or anything else.

So, moving on to the next question, and the next question is about which needs could be addressed by having a Security Incident response team?

P: Information and cyber security incidents, that could be affecting on very wide level of services or could be very serious.

I: Alright, now the third question is what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: Ability to withstand stress, good interaction skills, systematic and analytic abroach to problems and persistence.

About technical skills, because the team is formed around many experts, it is important to have good knowledge about their own technology which they are representing in the team.

Good ICT knowledge, it would be good thing to not forget about legal side, because they often play a part in security incidents, data protection as well, and knowing the employment law.

I: Good points, finally we have free speech if you have something to say about this topic.

P: It would be good to have some sort of training included in the security incident response team, either organized exercises, either in test environments or organized by someone else, also smaller tabletop trainings.

Well planned security incident response plan plays an important role, which results in repeatable actions, a high-quality incident response plan would be a good thing to have.

Processes, roles, and responsibilities should be well set into the organization, at least to the persons that are taking part on resolving security incidents.

I: Alright, good findings, thank you for taking the time to participate in this interview and have a nice rest of the day.

Appendix 7. P7 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section.

Both sections have 3 questions and after that is a free speech if there is time left for that. The first question is coming from security incident management process and is could you describe the different stages that are part of the current security incident management process?

P: Alright, my view for this is that the first stage is preparation, some thought has to be put into this in advance, policies and how to act. Try to identify critical systems in our own infrastructure and how to prioritize them, might vary a bit in customer work.

Then the second step would be detection and monitoring, monitoring impulses that are produced by our security products in use as well as announcements from Traficom and other global operators. Then opening tickets when it is necessary.

Third phase is analyzing, in this phase we already have a ticket, for example about some CVE and we analyze how it affects us or our customers. Also, this phase includes analyzing the inputs that are coming from those security products, reacting accordingly if it is needed.

If the reaction is needed, then the next phase is mitigation, where we are trying to restrict any further damages and try to contain the impact. If this is something server related, then it usually goes to other teams for handling as they have best know-how on their technologies if something has to be mitigated or isolate from network.

Then the fifth phase, removal, this means that for example if there is a CVE then there is a fix for it that is implemented, or if there would be a data breach then it is to be thought if it should be restored from backup or what the best solution might be to remove the threat.

Then the final phase is post incident, where the case should be gone through and see what happened, could some actions be improved in the future and so on. I am not quite sure if these are the official phases, but these are the ones that I thought that there might be.

I: Yes, very thoroughly answers, next question is if you could name 1-3 phases that you should be developed more?

P: Analyzing and post incident phases.

I: Ok, then the third question about this theme is could you tell me why you chose these stages in more detail?

P: Analyzing especially between external services, after the threat or vulnerability has been identified, in some cases the actions are not done in proper way. Then post incident phase, in cases that are for our own infrastructure, we can learn things in a proper manner, but in other environments the same mistakes are being made.

I: Alright, thank you, now we can move towards the next theme, which is security incident response team and the first question is just as simple as could you define what is security incident response team?

P: In our case it is a virtual team that mostly is first response to the case, handles the communications inside the organization and authorities and manages the responses to the incidents, also handles the relations towards our security product suppliers. Rarely does anything technical actions if personal computers don't count. Aims to make sure that case has been resolved and normal operations has been achieved as soon as possible.

I: Okay, now I have been giving participants a so-called textbook definition of a SIRT after they've given me their answers, so security incident response team is a team that handles identified security incidents. Now the next question is that which needs could be addressed by having a Security Incident response team?

P: Well, I think the most important thing is that proactive approach, that we have policies and tools before any incidents even have occurred in the first place. Then the probability of something happening is much lower. Second thing is that it allows faster reaction and handling of the incidents, if these would just come as a tickets from a single specialist, then this wouldn't be very fast or efficient.

Also making sure that we are complying in the regulations and understanding what requirements there are is also one important thing, as well as giving information to others as well.

I: Good points there, now the final question is what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: I feel like the most important thing is a good communication and group activity skills. Basic understanding on technologies is enough, because you just need to be able to assess the situation and how it affects on us and how we should delegate tasks towards different technology teams.

Technology knowledge can come directly from production groups, it doesn't necessarily have to be part of our security team. Also, not really a skill or talent, but there should be mandate to gather needed resources from different teams when it is necessary, it has been a problem in the past, but now it seems to be working rather well.

I: Okay, good skills that you mentioned there, nothing to argue with those. Now we are basically done with the questions, and there is still time left for free speech around this topic if you have anything in mind you would like to add or say.

P: Well, I think we should be able to develop our customer side, we are doing pretty good in our own infrastructure, but the same principles should apply towards the customers. Of course, there

is that problem that customer might not really want to pay for such services that kind of money that it would be beneficial for us to even produce such service, but at least some basic level security stuff.

I: So maybe there isn't such a suitable service even in our catalog at this moment that would answer to those needs?

P: Yeah, well we have some tailored services available for some customers.

I: So do you think we should develop some kind of new service like that, which we then could offer to our customers or do you mean that it should be implemented in general to our day to day work?

P: Maybe a bit of both, some part of it could be in our day-to-day operations because it doesn't really add too much to it, and some other parts could be sold as a managed service or something like that. I feel like many customers would be open for that kind of service.

I: Well thank you for finding the time to participate in this interview and have a good rest of the day.

Appendix 8. P8 Transcript

I: Interviewer

P: participant

I: So, questions are coming from two different themes, the first one is focused on security incident management process and later one is focusing on security incident response team section.

Both sections have 3 questions and after that is a free speech if there is time left for that, and the first question is could you describe the different stages that are part of the current security incident management process?

P: I would say that it goes into about five different phases. First it is observation of the incidents, depending of course the technology where the observation comes. Then second phase would be prioritizing those findings, how serious or critical these incidents are and the amount of those incidents. Then maybe like how many of those incidents are coming from one specific customer or system, then depending on those facts it is decided if it should be prioritized with a lower threshold.

Third phase would be interpretation of the incidents, here our first response team gathers the facts about what has happened if the alarm is indeed real or not. Based on interpretation, next phase would be that reacting to the incident, where the incident is investigated more thoroughly, and possible actions are then taken.

Finally, there is closing the incident, documenting necessary steps on what happened and what was done to resolve the incident. So, these five phases are that I would think of.

I: Alright, very good steps there, next question is if you could name 1-3 stages that you think should be developed more?

P: The most important thing is the closure that should be developed, documentation should be more clear and thorough on what has happened and what actions were taken, so if someone else would read these cases these things should be able to understand what was happened and what actions were taken. There are many cases where the documentation is not properly made, and people can't really understand what actions were taken and then one has to investigate it again to gain understanding. Or if later incident occurs, it should be possible to revisit the older incidents and see if there are any correlation between these cases.

Then the second thing I think is the interpretation of the incident should be improved as well, cases should be able to identify independently more efficiently. This would avoid so called unnecessary investigation made by multiple people and therefore would enhance the case handling. There are often cases where the handler is asking some information from someone else, and that information should have been able to figure out on their own in the first place, this leads to unnecessary mail or message threads and takes time from focusing on different matters.

Our number of personnel haven't been growing based on the amount of customers, so we are getting more and more customers and we have to handle the tickets with the same amount of personnel as before.

I: Okay, now the third question would be that if you could tell in more detail why you chose these stages, but those reason pretty much came out in your answers already, but if you have anything else to add?

P: Well, I think that was all.

I: Then we can move forward, and we can start with the security incident response team questions, and the first question is can you tell me what is a security incident response team?

P: Quite a wide question, but if I try to keep the answer short and compact, then security incident response team is a team that handles the interpretation of the incidents and how those incidents are being handled and handles the communication about those incidents as well.

I: Well said, we are pretty close to even my own textbook definition that I have been giving participants after they've given me their answers, so security incident response team is a team that handles identified security incidents. So, the next question is about which needs could be addressed by having a Security Incident response team?

P: Well, it is responsible for sufficiency, so the needed actions have been taken and maintaining the systems in use, so they don't get too old, or if some new and better system comes up those old systems can be replaced by the new ones. Then there is also that around the organization every system is available and accessible without a proper reason of doing so.

I: Okay, very good, then the third question is what skills would you consider required for the well-functioning security response team, these skills could be either technical or non-technical skills?

P: General knowledge on cyber security, as well as technologies that are related to cyber security, not meaning that one should know every product on some security organization but know a more general level what kind of products there are and what do they do. Overall knowledge on cyber security means that one should know what kind of threats there could be, it is easy to teach someone some specific products or systems after that.

Then it would be beneficial to know all the different operation systems, windows, Linux, Mac. Some kind of knowledge would be in order so one could understand how they work and what is happening, without that knowledge it is hard to decide whether the tasks it is performing are normal or not and what is the actual status of that system.

Then one of those non-technical skills that would be good to have, is an understanding the organizational structures, as this affects on how fast the tasks could be delegated to correct teams. So, these three things I came up with.

I: Okay, good skills you brought up, now that is all with the questions. Finally, we have some time left for free speech around this topic if you have anything in mind.

P: Well, something in general about cyber security is that there is a constant need for new experts, the need isn't really going down, it is in fact the opposite, the need for cyber security experts is growing all the time. The problem is really a global problem as there just isn't enough of professionals on the field. So, there is a need for experts to these jobs that would allow faster reactions and handling of the incidents. Without proper amount of experts those incidents just stay in the pipeline way too long because the experts don't have enough time to handle every ticket in time.

I: How do you feel, how should this problem be solved? Should the schools improve their teaching in the field of cyber security, or should there be more training within the organizations for those who are interested in cyber security?

P: Well, I think that schools should try to make this education more interesting. I feel like in university the teaching of this subject is very high level and theoretical, there should be more practical training and knowledge as well. Well, this didn't really answer on how to get more experts, but a bit about the education.

I don't really have a good answer on how to get more experts to this field, as the cyber security is very complex field, and one cannot really learn this that fast.

I: Yes, I feel like one could learn some specific thing quite fast, but to gain overall understanding of the field you should know about different operation systems, how the basic network is working and so on, it takes time to gain such level of knowledge. Also, there are those non-technical skills that come also along the way.

P: Yeah.

I: But yeah, good points there, and now I thank you for finding the time to participate in this interview, as there aren't that many participants all of your answers matter to gain as much data as possible.