Bachelor's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Jo Thorsen Håndstad
Petar Ilic
Sindre Logstein

Components to Establish a CSIRT Environment

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Erjon Zoto
May 2023

NTNU
Norwegian University of
Science and Technology

Jo Thorsen Håndstad
Petar Ilic
Sindre Logstein

Components to Establish a CSIRT Environment

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Erjon Zoto
May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

Title:	Components to Establish a CSIRT Environment
Date:	22.05.2023
Authors:	Jo Thorsen Håndstad
	Petar Ilic
	Sindre Logstein
Supervisor:	Erjon Zoto
Task giver:	Raymond Hagen, Digitaliseringsdirektoratet (Digdir)
Keywords:	CSIRT, COMPONENTS, SRM, DIGDIR, IRT
Pages:	76
Attachments:	10
Availability:	Open

Abstract: In a world where cyber threats are increasingly sophisticated and widespread, CSIRTs (Cyber Security Incident Response Teams) play a crucial role in protecting us against digital attacks. The Norwegian Digitalisation Agency has explored the idea of establishing its own CSIRT for their common solutions and has tasked the group with researching the necessary components required for this endeavour. Therefore, the research question is as follows: *What are the necessary components needed to establish a well-functioning CSIRT?* To answer this question, a literature study based on a framework developed by FIRST was conducted. The result is a proposed CSIRT environment with components capable of supporting every function outlined in the FIRST framework.

Sammendrag

Tittel:	Komponenter til å etablere et CSIRT-miljø
Dato:	22.05.2023
Deltakere:	Jo Thorsen Håndstad
	Petar Ilic
	Sindre Logstein
Veileder:	Erjon Zoto
Oppdragsgiver:	Raymond Hagen, Digitaliseringsdirektoratet (Digdir)
Stikkord:	CSIRT, KOMPONENTER, SRM, DIGDIR, IRT
Antall sider :	76
Antall vedlegg:	10
Publiseringsavtale:	Åpen

Sammendrag: I en verden der cybertrusler blir stadig mer sofistikerte og utbredt, spiller CSIRT, Cyber Security Incident Response Team, en avgjørende rolle i å beskytte oss mot digitale angrep. Digitaliseringsdirektoratet har utforsket ideen om å etablere sin egen CSIRT for sine fellesløsninger, og har gitt gruppen i oppgave å undersøke hvilke komponenter som kreves for dette. Problemstillingen er derfor som følger: *Hva er de nødvendige komponentene som trengs for å etablere en velfungerende CSIRT?* For å finne svaret på dette, ble det gjennomført en literaturstudie med utganspunkt i et rammeverk utviklet av FIRST. Resultatet av dette er et foreslått CSIRT-miljø med komponenter i stand til å støtte alle funksjonene i FIRST-rammeverket.

Preface

We would like to thank our task giver Raymond Hagen for providing a highly relevant and engaging task. His support and guidance has played a significant role in our achievements, and we are confident that the knowledge we have amassed from him, as well as the task, will greatly contribute to our future professional endeavours. We would also like to express our gratitude to our supervisor, Erjon Zoto, who has provided helpful feedback throughout this project.
Finally, we would like to express our gratitude to Reidar Mouhleb and NCSC for providing us with valuable insights, and welcoming us to their headquarters in Oslo. We truly appreciate the time you dedicated to us and our matter.

Contents

Figures

Tables

Acronyms

AI Artificial Intelligence. 14, 19

API Application Programming Interface. 18, 62

APT Advanced Persistent Threat. 11, 12

CERT Computer Emergency Response Team. 9, 10

CSIRT Computer Security Incident Response Team. 2–5, 7–13, 16–21, 24–27, 29, 31–39, 41–56, 58–68, 71, 76

CSV Comma-separated values. 49

DDoS Distributed denial-of-service. 15

ICT Information and communications technology. 9

JSON JavaScript Object Notation. 49

NIST National Institute of Standards and Technology. 10, 20, 47

NSM Nasjonal sikkerhetsmyndighet (The Norwegian National Security Authority). xiii, 7–9

OSINT Open-source intelligence. 11, 15

SIEM Security Information and Event Management. 13–15, 17, 19, 30, 32, 33, 42–45, 47, 55, 56, 60

SOC Security Operations Center. 9, 10, 36

Glossary

ad-hoc Something that is created or done for a specific purpose or situation, typically without prior planning or formal structure. 34

artefact Any piece of information or evidence that is extracted or recovered from digital devices or systems. E.g., files, metadata, logs, network traffic, registry entries, timestamps, and user-generated data. 33, 34, 58, 59

brute-force A method used in cybersecurity where an attacker systematically tries all possible combinations or passwords to gain unauthorised access to a system or data. 15

common solutions Refers to the services that Digdir provides. These solutions focus on functionality and user friendliness, by allowing users (residents) to use these solutions across administrations. Eg., ID-porten, which offer residents the same login functionality regardless of agency and municipality . 1, 2

constituent An entity or organisation that seeks assistance or guidance from the CSIRT regarding a potential security incident. 8, 13, 17–20, 33–39, 42, 44, 47, 48, 52–54, 56, 58, 61–66, 68, 71

glitch A temporary or unexpected malfunction or error that causes a deviation from the expected behaviour or functionality of a program or system. 16

machine learning A field of artificial intelligence that involves developing algorithms and models that enable computers to learn from data and make predictions or decisions without explicit programming. 15, 53

middleware Software that acts as a bridge or intermediary between different applications, systems, or components to facilitate communication and data exchange. 18

phishing The practice of deceiving individuals or organisations into divulging sensitive information, such as usernames, passwords, or financial data, by posing as a trustworthy entity in electronic communications. 15, 16, 46

REST API An Application Programming Interface which enables communication and interaction between systems over the internet using standard HTTP methods. 44, 48, 49, 60, 64

SNMP trap Used to notify the SNMP manager about specific events or conditions that occur on the SNMP-enabled devices, such as system failures, performance degradation, network errors, security breaches, or other significant events that need attention. 18

spoof intelligence Information related to the identification of sources behind domain spoofing attempts. 46

syslog A standardised protocol used for message logging, allowing devices and applications to send event notifications to a central logging server. 18, 44, 49, 52, 53

Trojan horse A type of malicious software that disguises itself as a legitimate program to deceive users and gain unauthorised access to their systems or steal sensitive information. 12

Ubuntu An open-source operating system based on the Linux kernel and Debian architecture. 58

Chapter 1

Introduction

"*Information security should be a part of every digitalisation project in public administration from the beginning, and throughout the entire life cycle of the system. The goal is to reduce the number of vulnerabilities and to ensure that digital services are reliable and robust. By taking this into account already during development and procurement, information security can be cost-effectively integrated into the solutions. The directorate is responsible for ensuring that this happens in connection with the operation and development of its own common solutions.*"
– The Royal Ministry of Local Government and Regional Development, 2023[1]

1.1 Background

The Norwegian Digitalisation Agency is a Norwegian state directorate that aims to develop and improve the digitalisation of the public sector. With offices in Brønnøysund, Leikanger and Oslo, they oversee services including Altinn and ID-Porten, among other public services. As with any organisation, The Norwegian Digitalisation Agency is looking for ways to bolster their security posture, specifically in the field of incident handling.

From this point forward The Norwegian Digitalisation Agency will be referred to as "Digdir".

1.2 Project Area

In this section, we introduce the project area, including the problem area, problem statement, problem delimitation, and the chosen framework. These elements provide a clear understanding of the project's context, core issue, boundaries, and strategic approach.

1.2.1 Problem Area

Two years prior to this report, Digdir received a request from the Ministry of Local Government and Regional Development. The ministry requested a development to be made in incident handling. Based on this request, Digdir have explored the possibility of establishing their own CSIRT department for their common solutions[1]. The objective of this report is to support Digdir in this endeavour with relevant and reliable information as to the components required to establish a CSIRT environment.

1.2.2 Problem Statement

We have been tasked with providing Digdir with a framework/portfolio on how to establish a CSIRT, with the focus being on the various components that are needed. As a large government agency handling enormous amounts of data, including sensitive information that could be of interest to malicious actors, establishing a CSIRT would be a sensible addition to Digdir's security operations. Thus the research question is as follows: *What are the necessary components needed to establish a well-functioning CSIRT?*

The proposed solution to establishing the CSIRT will include components, which are both hardware and software tools, that are able to optimally secure Digdir's infrastructure, as well as the processes and competence that is required in order to effectively operate a CSIRT.

1.2.3 Problem Delimitation

The proposed components will rely on thoroughly sourced and dependable data. The selection process has deliberately focused on utilising a singular framework, namely FIRST CSIRT Services Framework 2.1.0[2]. Within the FIRST framework, the primary emphasis will be directed towards the Service Areas (1.2.4), aiming to identify appropriate solutions based on the functions these contain.

As the researchers are not able to conduct their own testing, the proposed components to establish the CSIRT are therefore based on reliable information found through various sources, coupled with the researchers own critical thinking and decision making strategies. Tools that have been recently developed and lack substantial information or reviews will not be taken into consideration, as their limited availability of information restricts their suitability for the research purposes.

1.2.4 Framework (FIRST)

In order for Digdir's CSIRT to provide optimal security, the research will follow a specific framework. This will be the FIRST CSIRT Services Framework[2]. The

[1] `https://aarsrapport2021.digdir.no/kapittel-3/status-pa-oppdrag-i-tildelingsbrev/61`, visited 29.03.2023

FIRST framework is divided into sections known as *Service Areas*:

1. Information Security Event Management
2. Information Security Incident management
3. Vulnerability Management
4. Situational Awareness
5. Knowledge Transfer

The research will systematically follow these service areas and their respective functions, aiming to optimise the level of protection that the CSIRT will be capable of delivering. The FIRST framework will be further discussed in Section 3.3 and Chapter 4.

1.3 Target Groups

This section provides the reader with the relevant target groups for the report. The target groups are the categories of individuals or organisations in which the report may be relevant, meaningful or influential to.

1.3.1 The Norwegian Digitalisation Agency

The main target group for this report is Digdir. As a government agency responsible for multiple digital solutions concerning national identification and access to public services, being able to handle and prevent cyber security incidents is vital. The report is aimed to present Digdir with a proposed architecture and a portfolio on how a CSIRT environment could look like based on current technologies.

1.3.2 CSIRTs in General

While Digdir is the main target group, other parties could also benefit from the findings in this report. This could be other government agencies or private companies and organisations with the need and necessary resources for a CSIRT, or already established CSIRT's looking to improve their operations.

1.3.3 Others

The findings presented in this report can be of value to various other parties beyond Digdir and CSIRTs. For instance, researchers and students with an interest in incident response can benefit from the insights provided herein, as well as those seeking additional documentation to support their own research purposes.

1.4 Researchers' Background

The research group consisted of three members - Jo Thorsen Håndstad, Petar Ilic and Sindre Logstein. The researchers shared a common professional background and were all in their final year of their Digital Infrastructure and Cyber Security studies at NTNU in Gjøvik. Other than a few exceptions, the group mostly shared the same curriculum and had selected the same electives. A subset of the courses taken were considered to be more applicable to the research than others, notably: Risk Management (DCSG2005), Software Development (PROG1004), as well as various networking courses (DCSG1006/2001 & IIKG3021).

1.5 Reasons For Choosing The Task

Due to limited prior experience in the realm of CSIRTs and the associated tools used to establish them, the researchers wished to expand their knowledge in this area. The creation of a CSIRT holds significant importance within the context of incident response. By successfully undertaking this task, valuable expertise will be acquired, which can subsequently be applied in real-world scenarios.

1.6 Project Framework

With the project start in January 2023 and a delivery deadline the 22nd of May 2023, the researchers had a limited time frame to acquire relevant knowledge, conduct research, and write the report. The organisation of time was therefore a crucial aspect in facilitating an effective work process, and was planned through the use of a Gantt chart (Appendix C). The Gantt chart provides a clear visualisation of how the project was scheduled. Notably, 9 weeks was allocated to conduct the research.

1.7 Project Roles

Extensive research was necessary due to the multitude of components and their diverse distributors. To ensure a comprehensive solution, task distribution among team members became imperative. Given the absence of prior knowledge, it was crucial for each member to acquire a foundational understanding of every component involved. Furthermore, all components are interrelated and complement one another in various ways. As a result of task distribution, every team member gained knowledge about each component, and we were able to engage in discussions about the differences between them to identify the optimal solution.

Our supervisor, Erjon Zoto, held weekly meetings with us in which he provided guidance on various aspects of the project. Specifically, his responsibilities included advising on the project's structure, outlining the requirements for docu-

mentation, overseeing the execution of the project, reviewing the completed tasks to ensure consistency, and offering assistance with relevant academic inquiries.

Raymond Hagen was our task giver and was representing Digdir. Meetings were held with Raymond on a weekly basis, during which he provided guidance on the project. Specifically, Raymond addressed inquiries related to the task and provided guidance on structuring the thesis according to the chosen framework. Due to his expertise with various tools, he also assisted in understanding the functionalities and interrelationships of the tools. Questions were posed to Raymond either during the weekly meetings or via the Teams room. As such, Raymond's role was to facilitate comprehension of the task at hand, as well as the various concepts, components, and tools associated with a CSIRT.

1.8 About The Report

The chosen language for the report is English, and it is written in Overleaf, an online LaTeX editor. The report contains a glossary, as well as an acronym list. By hovering over foreign words, it may be further explained in the glossary. This also applies to frequently used acronyms, or acronyms that are not otherwise explicitly explained in the text.

As previously stated, the components that will be presented include tools of both hardware and software. Consequently, the terms "components" and "tools" will be used interchangeably throughout the report.

1.8.1 Report Structure

The report consists of 7 chapters that will cover these main topics:

- Necessary theoretical material
- Methodology and the approach used by the researchers in undertaking the task
- Detailed overview of the FIRST framework
- The solution, discussion of relevant topics, and summary and possibilities for further work

Chapter 2

Theory

This section will explore and explain key concepts relevant to the thesis, to provide a comprehensive understanding of the research. Additionally, the background of why CSIRTs are essential to organisations will also be explored.

2.1 What is a CSIRT?

CSIRT stands for Computer Security Incident Response Team and it denotes a crucial element for modern organisations. An IT department is not enough to secure the digital infrastructure as cyber security threats constantly evolve, making it impossible for the IT department to anticipate and prevent every possible attack. A CSIRT is better equipped to respond to new and emerging threats as they arise.

It is a common misconception that a CSIRT belongs to an organisation's IT department. To fully comprehend the goals and objectives of a CSIRT, it is crucial to recognise why this assumption is inaccurate. The IT department plays a critical role in an organisation's daily operations, whereas the CSIRT is a specialised resource that is called upon as necessary, especially in cases of significant security incidents[3]. In these situations, the organisation can rely on the CSIRT's guidance, competence, and expertise to effectively mitigate threats. It is also important to note that in the context of this thesis, the use of the term CSIRT may differ from the usage found elsewhere. In this case, CSIRT is used synonymously with NSM's definition of SRM (Norwegian: Sektorvise responsmiljø)[4]. The reason for this is that Digdir's size not only justifies them having their own CSIRT unit, but considering the broad spectrum of sectors Digdir oversee in their operations, they could act as an SRM (Appendix E).

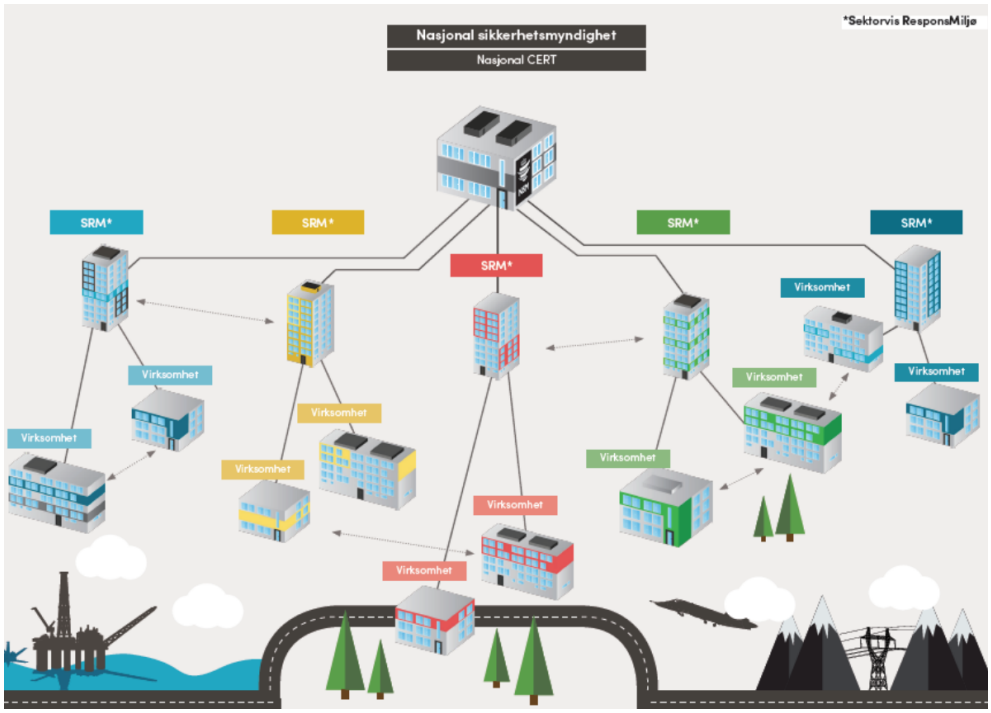


Figure 2.1: Relation between NSM, SRMs and organisations[4]

As Figure 2.1 shows, the relationship between NSM, SRMs (CSIRTs) and organisations is of a hierarchical structure. At the top is NSM, which acts as a national CSIRT with direct communication to the other sector-wise CSIRTs, located at the middle level of the structure. At the base are the organisations, which function as clients with direct communication to their corresponding CSIRT. In addition to vertical communication among the constituents, sector-wise CSIRTs and organisations engage in lateral communication among themselves. These correlations play a significant role in the knowledge transfer service area, which will be further discussed in Section 4.4.

2.1.1 What Does a CSIRT Do?

A CSIRT has various roles and responsibilities when it comes to securing an organisation's digital assets. The *"Handbook for Computer Security Incident Response Teams (CSIRTs)"* drew a clever analogy between CSIRTs and fire departments. The same way a fire department is called in a fire emergency, a CSIRT is contacted in cases of security incidents[5]. An important takeaway from this analogy, is that a CSIRT's main task is to respond to serious security incidents, as a routine in an emergency.

When a CSIRT responds to a security incident, it is mainly done through guidance. When an incident occurs, the CSIRT will have all the necessary data and

information that is needed on the organisation in order to provide effective aid. This includes the organisation's infrastructure, logs and overall security posture. However, with this large amount of data, the CSIRT can also notify constituents about potential security incidents, rather than only being a one-way resource. Furthermore, the CSIRT is involved in the entire incident response cycle. According to NSM's framework for managing ICT security incidents, a CSIRT's job can be broken into six distinct parts[4]. These are:

- Planning and preparation
- Detection and assessment
- Notifying
- Implementation of processes and measures to handle the incident
- Situational reporting
- Recovery and learning from the incident

In other words, a CSIRT is involved before, during and even after security incidents. Through planning, preparation, detection and assessment, the CSIRT improves an organisation's readiness before an incident occurs. Through notifying and situational reporting, the CSIRT strengthens an organisation's ability to mitigate and respond to incidents. Lastly, the CSIRT assists organisation's in post-incident recovery and facilitates a valuable learning process by conducting evaluations and providing guidance on future measures.

2.1.2 CERT & SOC vs CSIRT

Gaining insights into the responsibilities and capabilities of various cyber security teams is beneficial, considering that the solution will incorporate elements from other incident response teams. Two additional types of cyber security teams, namely CERTs and SOCs, will be further explained as they also play a pivotal role in protecting an organisation's information systems from cyber threats[6].

A CERT is a team of experts responsible for providing proactive and reactive services related to cyber security incidents and vulnerabilities[1]. The primary focus of a CERT is to identify, analyse, and respond to cyber security threats and vulnerabilities before they can cause significant damage to an organisation's systems and data. Their primary duties include[2]:

- Identifying and analysing cyber security threats and vulnerabilities that could affect the organisation
- Providing guidance and advice to the organisation's IT and security teams on how to mitigate the risks associated with identified threats and vulnerabilities

[1] See: `https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert`, visited 13.03.2023

[2] See: `https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team`, visited 13.03.2023

- Developing and disseminating security best practices and guidelines to help organisations prevent cyber attacks
- Coordinating with other CERTs and security organisations to share threat intelligence and collaborate on incident response

A SOC is responsible for maintaining the security of an organisation's network and systems on a 24/7 basis. The primary focus of a SOC is to proactively detect, prevent, and respond to cyber threats before they can cause significant damage to the organisation's systems and data. SOCs are typically staffed with security analysts, threat intelligence specialists, and other IT professionals with the primary goal to identify and respond to security incidents[3]. Additional responsibilities encompass[4]:

- Monitoring the organisation's network and systems for security threats and incidents
- Analysing and investigating security incidents to determine their cause and extent
- Implementing security controls and policies to prevent and mitigate the risks associated with identified threats and vulnerabilities
- Coordinating with other teams, such as CSIRTs and CERTs, to respond to security incidents and ensure business continuity
- Conducting threat intelligence analysis to identify new and emerging threats and vulnerabilities

In summary, even though their responsibilities may overlap, CSIRTs, CERTs, and SOCs are all critical components of an organisation's cyber security strategy. CSIRTs focus on assistance and guidance, CERTs focus on identifying and mitigating cyber security threats and vulnerabilities, and SOCs focus on proactively monitoring and maintaining the security of an organisation's network and systems[5].

2.2 Threats

There are several threats an organisation has to defend against in the modern world. According to NIST, threats are defined as an event with the potential to negatively impact organisational operations by the means of unauthorised access, destruction, disclosure, or modification of information, and/or denial of service[6]. The threat actors are the individuals or groups posing a threat[7].

[3] See: `https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities`, visited 14.03.2023

[4] See: `https://www.techtarget.com/searchsecurity/tip/5-key-enterprise-SOC-roles-and-responsibilities`, visited 14.03.2023

[5] See: `https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference`, visited 16.03.2023

[6] See: `https://csrc.nist.gov/glossary/term/threat`, visited 06.04.03.2023

[7] See: `https://csrc.nist.gov/glossary/term/threat_actor`, visited 06.04.2023

Threat actors usually look for vulnerabilities to exploit rather than focus on specific organisations or individuals, as they are opportunistic and often move on if the target appears to exhibit robust security measures. Digdir can be described as an organisation with valuable information, as a result, Digdir faces well-funded groups such as APTs, which will be the focus of the present section[8] .

2.2.1 Advanced Persistent Threats

APT stands for Advanced Persistent Threat and is a term used to describe a prolonged and targeted cyber attack[7]. The deployment of an APT demands significant resources and an exhaustive planning process. Hence, the selection of targets primarily hinges upon the potential value of information that can be procured or how much damage it can cause an organisation or country[8].

High valued information might include intellectual property or personal/-sensitive information. Digdir, which is a merger between Altinn and Difi, is a high valued target as it is responsible for large amounts of sensitive information to provide important public services[9].

2.2.2 APT Attack Methods

It is important to comprehend how an APT operates, as doing so allows for a better understanding of the requirements for protection against such attacks. This knowledge highlights the inadequacy of standard defences and emphasises the necessity of specialised organisations such as CSIRTs.

The main reason that standard defence components, such as firewalls and antiviruses are inadequate, is that APTs will try and stay hidden. This means attacks won't use methods that can be detected such as deploying malware. CrowdStrike's global threat report shows that 71% of cyber attacks are malware free in 2022, making it impossible for signature-based detection systems to detect[9]. Furthermore, attackers may deactivate defensive measures and detection mechanisms subsequent to infiltrating a network[8].

Information gathering on the target is crucial for the attacker, as the organisations typically have robust security measures. An attacker will usually utilise OSINT tools to gather information on the organisations and its employees, as this approach tends to evade detection and avoid raising suspicion[10] . In the event that OSINT fails to yield sufficient information, APT groups resort to utilising active tools to extract information relevant to domains, ports, and IP addresses in use, as well as the software programs within the target's infrastructure[11].

[8] See: `https://www.fortinet.com/blog/ciso-collective/top-security-threats-for-government`, visited 06.04.2023

[9] See: `https://www.digdir.no/digdir/about-norwegian-digitalisation-agency/887`, visited 08.04.2023

[10] See: `https://www.cyber.airbus.com/apt-kill-chain-part-3-reconnaissance/`, visited 03.04.2023

[11] See: `https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/`

The subsequent stage involves obtaining an initial point of entry, which may be achieved through three primary routes: web-based assets, network resources, or authorised human users. This is done by using methods such as social engineering and malicious uploads[7]. KnowBe4 reports that spear phishing is responsible for 91% of successful cyber-attacks[12]. The purpose of this stage is to covertly install a backdoor or Trojan horse on a computer within the network[10].

The attacker will subsequently attempt to escalate their network access, unless they have acquired sufficient reconnaissance data to precisely identify the specific endpoint containing the desired information. However, it is more likely that this is unknown to the attacker, and that further reconnaissance and broader attacks are necessary to locate the valuable data[10]. The attacker will therefore need to move lateral through the network while staying undetected. This means gaining access to more systems and users. The attacker is unlikely to successfully exploit known vulnerabilities, as such actions would trigger alarms, which would alert security personnel. They will therefore resort to stealing or guessing passwords based on what they learned from the initial entrypoint[13]. Another method to broadening their access is to find forgotten files or bad configuration in programs[14]. The final step of the attack involves the extraction of the stolen data and the removal of any evidence of the intrusion. Attackers may use diversionary tactics to distract or hinder security personnel while attempting to cover their tracks[7].

2.2.3 Defending Against APTs

Organisations that are targeted by APTs face significant challenges in detecting and responding to these attacks. Traditional security measures such as firewalls, antivirus, and intrusion detection systems may not be sufficient in detecting and preventing APT attacks. Most attacks follow the pattern described in the prior section and can therefore, with enough data, be recognised. A CSIRT, which has the ability to perform extensive traffic monitoring and log gathering, is well-equipped to detect and analyse such attack patterns, enabling timely response and mitigation measures to safeguard an organisation's digital assets and infrastructure.

2.3 Components

A CSIRT relies on a wide range of components in order to function properly and effectively. These components will assist the CSIRT to gather information, organise and triage useful information, communicate with partners, and do forensic

[12] `https://www.knowbe4.com/spear-phishing/`, visited 03.04.2023

[13] `https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement`, visited 04.04.2023

[14] See: `https://www.cyber.airbus.com/apt-kill-chain-part-5-access-strenghtening-lateral-movements/`, visited 03.04.2023

analysis to understand malware. Furthermore, CSIRTs must actively gather intelligence on emerging vulnerabilities, stay informed about the latest updates, and proactively develop robust countermeasures that can be efficiently deployed across their constituents' infrastructures to effectively mitigate potential risks[6]. The following sections will delve into the theoretical aspects of some of the components and why they are crucial for a CSIRT.

2.3.1 Security Information and Event Management

SIEM stands for Security Information and Event Management, and it stands at the centre when it comes to a CSIRT's ability to perform its responsibilities. It is a solution that provides real-time visibility into the activities and events occurring within an infrastructure, enabling monitoring of ongoing activities and accessing logs of historical events[15]. To do so, a SIEM will review data collected from a large number of sources. SIEMs have evolved from being a component that helps organisations comply with industry security regulations, to a component with a range of capabilities including response, investigation, and detection[11]. A SIEM can be deployed either on-premises or in the cloud, with each option having its own set of benefits and drawbacks. An advantage of a cloud-based SIEM is that the cloud provider will have a team ready to support, maintain and configure the SIEM, and therefore there is no delay in deployment because of the need to train personnel. However, there are some drawbacks to cloud based SIEM. Examples include, sensitive data will be moved off site and there is always an associated risk with moving data[16].

It is essential to have a basic understanding of how a SIEM operates to appreciate its value. As mentioned earlier, a SIEM operates on vast amounts of data that are beyond human capacity to manage. A SIEM will consequently use logs to generate alerts that it deems significant and requires human attention. To make the alerts more manageable, a SIEM aggregates and correlates data from multiple sources[11]. Data aggregation is taking similar events and turning them into one event. For example, a user connecting to a server will create multiple logs on a router - logs that mostly look the same. Aggregation can summarise those into one event, while data correlation can find relationships between events that appear seemingly unrelated[17]. Furthermore, complementary concepts within a SIEM system, that supports and supplements its capabilities will be explored, including XDR, SOAR, TIP and UEBA. A SIEM that is integrated with these components might also be called a "Next-Generation SIEM", as it has evolved from a simple log monitoring and managing solution[12].

Alternative security components are available to organisations that may not have the resources to implement a SIEM or require security needs beyond the

[15] `https://www.atatus.com/glossary/siem/`, visited 17.04.2023

[16] `https://www.exabeam.com/explainers/next-gen-siem/cloud-siem-features-capabilities-and-advantages/`, visited 17.04.2023

[17] See: `https://www.peerspot.com/questions/what-is-the-difference-between-it-event-correlation-and-aggregatio` visited 17.04.2023

scope of a SIEM. One such alternative is XDR, which stands for Extended Detection and Response. XDR combines NDR (Network Detection and Response) and EDR (Endpoint Detection and Response) into a single component. XDR can therefore be described as a component for detecting, containing, and responding to cyber threats[13]. During the research, the team has discovered that security software companies have varying definitions for XDRs and SIEMs, but most of them use them interchangeably as SIEMs also have NDR and EDR capabilities. In addition, SIEMs also have the capabilities to monitor compliance with industry regulations, data retention and reporting[13].

2.3.2 Security Orchestration and Response

SOAR or Security Orchestration and Response, is a tool that allows organisations to automate and streamline their security operations. SOAR does this by leveraging playbooks, which are pre-configured and automated response actions that are triggered when specific conditions are met. SOAR solutions will make use of AI to prioritise incidents, and subsequently take the appropriate course of action. This will lower response times on common security incidents, as well as the amount of events a human will have to manage. For example, a SOAR can automatically detect suspicious activity and initiate actions such as quarantining a device. By taking immediate automated actions, SOAR can help prevent the spread of malware and stop insider attacks in its starting phase, minimising the impact of a potential attack[18].

Given a SOAR's immediate and direct response capabilities, they are not directly applicable to a CSIRT's operations (2.1.2). However, they are an essential component to some SIEM solutions. A SIEM often relies on a SOAR for its response capabilities and it is part of what is referred to as a Next-Generation SIEM[12]. Like SIEMs, a SOAR also needs large amounts of data to create any meaningful impact on security. Therefore, a SOAR can make use of a SIEM's data collection capabilities. The SIEM will collect, correlate and send security events to a SOAR, which will then act based on the predefined playbooks[19].

2.3.3 Threat Intelligence Platform

A Threat Intelligence Platform (TIP) is a centralised solution that collects, manages, and analyses threat intelligence data from various sources to provide valuable insights about potential cyber threats. Using a TIP will facilitate the sharing of data with other teams such as analysts, security teams and management teams, enabling organisations to collaborate if an attack occurs[20]. The TIP will collect

[18] See: `https://www.techtarget.com/searchsecurity/answer/SOAR-vs-SIEM-Whats-the-difference`, visited 14.04.2023

[19] See: `https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/xdr-vs-siem-vs-soar/`, visited 14.04.2023

[20] See: `https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform`, visited 22.04.2023

and aggregate threat intelligence data from a wide range of sources such as OSINT, third parties, internal sources and Government Trusted Sharing Communities (ISACs)[14]. ISACs stands for Information Sharing and Analysis Centers, and are non-profit organisations providing and gathering vital resources on cyber security threat information[21].

The data collected by a SIEM, and the vast amount of data that a TIP has, are complementary to each other. This is because it allows a SIEM to compare data from internal systems with known threats, such as compromised IP addresses, domains or file hashes, and automatically mitigate attacks from these known risk sources[22]. By comparing data, a SIEM can also improve false positives as it will have more data to draw on, allowing it to better distinguish between legitimate events and potential security threats[14].

2.3.4 User and Entity Behaviour Analytics

UEBA stands for User and Entity Behaviour Analytics and is a type of security technology that focuses on detecting and analysing abnormal behaviour of users and entities within an organisation's network or system. SIEM suppliers have begun integrating UEBA into their solutions for improved threat detection[23]. The key components of UEBA typically involve behaviour modelling, anomaly detection, and risk scoring[24]. Behaviour modelling leverages machine learning on data from multiple sources to establish a baseline of typical behaviour for devices and users. Anomaly detection techniques are then used to identify deviations from these baselines, which may indicate potential security threats. Anomalies can be a user showing abnormal download patterns or multiple login attempts from an unknown IP address. Finally, risk scoring is applied to prioritise and flag potential security incidents based on the severity and relevance of the detected anomalies[25].

UEBA makes a network considerably more secure and brings many benefits to security. For example, UEBA will detect insider attacks that may bypass traditional security measures, providing organisations with enhanced threat visibility. Cyber attacks have evolved to target human fallibility through social engineering and phishing attacks, rather than exploiting technical vulnerabilities in the infrastructure. These attacks can compromise a single user or system, which can then be used as a foothold for a larger scale attack. UEBA is equipped to find those compromised systems and stop a potential attack, while also offering better protection against brute-force and DDoS attacks compared to a standard SIEM[26].

[21] See: `https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing`, visited 22.04.2023

[22] See: `https://www.exabeam.com/explainers/siem/threat-intelligence/`, visited 24.04.2023

[23] `https://www.technology.org/2019/04/30/siem-ueba-and-soar-whats-the-difference/`, visited 26.04.2023

[24] `https://www.exabeam.com/ueba/user-entity-behavior-analytics-scoring-system-explained/`, visited 26.04.2023

[25] `https://www.ibm.com/topics/ueba`, visited 26.04.2023

[26] `https://www.fortinet.com/resources/cyberglossary/what-is-ueba`, visited 27.04.2023

2.3.5 Vulnerability Assessment and Management

Vulnerability management encompasses the systematic procedure of identifying, assessing, mitigating, and documenting security vulnerabilities present within systems and the underlying software they rely upon[15].

Vulnerability assessment entails conducting a comprehensive assessment of the network within an organisation. The identified vulnerabilities are subsequently categorised into hardware, software, or human-related, after which they are prioritised, to guide the CSIRT in determining the order of remediation efforts. Hardware vulnerabilities include outdated firmware and devices, while software vulnerabilities refer to flaws, glitches, or weaknesses in the software code. The misconfigurations of hardware and software will significantly contribute to the occurrence of vulnerabilities[27]. Human vulnerabilities involve aspects such as weak passwords, engaging with malicious websites, and opening phishing emails[15].

To find these vulnerabilities the CSIRT can make use of penetration testing (pen testing) and vulnerability scanners. Pen testing is either conducted by ethical hackers or is automated and is the process of trying to exploit vulnerabilities in applications and systems[28]. Vulnerability scanners operate automatically and utilise a database, known as a vulnerability signature database. The scanner will examine whether the organisation's applications or systems possess any exploitable known vulnerabilities from the database. The scanner scans from both inside and outside the network. External tests are done from the perspective of an attack from outside the network, and will provide information on how the organisation will fare against external threats. Internal means the scanner will scan as a user inside the network with privileged access, and is relevant for information on insider threats[29].

2.3.6 Virtual Machines

A virtual machine (VM) is an operating system (OS) or application running as software on dedicated hardware, imitating the use of real dedicated hardware[30]. Simply put, it is a virtual machine running inside a physical one. VMs are a useful asset in digital forensics, as they provide a safe environment for forensic analysts to perform their necessary functions. In cyber security, these environments are known as sandboxes. In a sandbox environment, researchers and analysts can execute potentially malicious code without affecting other critical resources[31]. The insights gathered from a sandbox environment are crucial in understanding how

[27] See: https://www.hackerone.com/knowledge-center/what-vulnerability-assessment-benefits-tools-and-process, visited 02.05.2023

[28] https://www.techtarget.com/searchsecurity/tip/The-differences-between-pen-tests-vs-vulnerability-scanning visited 03.05.2023

[29] https://www.datamation.com/security/external-vs-internal-vulnerability-scans-whats-the-difference/, visited 03.05.2023

[30] See: https://www.techtarget.com/searchitoperations/definition/virtual-machine-VM, visited 19.04.2023

[31] See: https://www.proofpoint.com/us/threat-reference/sandbox, visited 19.04.2023

a security incident has affected a constituent's systems. Therefore, they are an integral component in the proposed CSIRT environment, regarding digital forensics.

2.3.7 Data Collection Techniques and Components

As previously exlpained, a SIEM is entirely dependent on data to perform its tasks. It should therefore collect data from as many points as possible[32]. Collecting every log from every device is usually not possible as this would require a large amount of resources. Therefore, a CSIRT should decide what infrastructure is business critical, and which can provide the SIEM with important security information[16]. Log collecting from too many points in the infrastructure can also lead to a SIEM reporting more false positives than desirable, which can lead to legitimate alerts getting buried[33]. Critical logs that warrant consideration include network logs, security control logs, and host logs[16].

Network logs are logs that describe the data flowing between endpoints inside the network and data flowing out of the network. The logs contain essential information regarding its origin, destination, and packet requests[34]. An Intrusion Detection System (IDS) is a highly effective component for the collection of network logs. IDSs come in two variants: Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS). A HIDS is installed on an endpoint and will detect anomalies on a host. NIDS on the other hand, scans the network at strategic points in the infrastructure and is the most effective component for gathering traffic information[35].

Host logs refer to the logs generated by endpoints in an infrastructure, such as servers and computers. These logs can encompass a range of information, including application logs, changes and sharing of files, and documents and system logs[36]. Security control logs are logs from the IDS and/or endpoint securities, such as an antivirus and firewalls[16].

There are also different methods used to collect logs. The two main methods are called agent-based log collection and agent-less log collection. Agent-based log collection requires agents to be installed on the host. These agents collect, filter, parse, and convert the logs into other formats before sending them to the log collection server. Benefits of using an agent includes[17]:

- Log filtering
- Collection from a wide range of platforms

[32] See: `https://medium.com/@pivotalsec/how-to-decide-which-data-source-to-collect-in-a-siem-e26316d1dfb8`, visited 21.04.2023

[33] See: `https://solutionsreview.com/security-information-event-management/what-generated-data-should-your-siem-ingest/`, visited 22.04.2023

[34] See: `https://www.manageengine.com/log-management/siem/log-netflow-collection-processing.html`, visited 22.04.2023

[35] See: `https://spanning.com/blog/intrusion-detection-systems-deep-dive-into-nids-hids/`, visited 22.04.2023

[36] See: `https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html`, visited 24.04.2023

- Secure and compressed log transfer
- Conversion of logs to make it readable for a SIEM

Agent-less log collection is when the device sends its logs automatically to a log collector without having an additional log agent installed. This approach may be employed on hosts that lack support for downloading supplementary programs, such as firewalls, printers, and routers. Routers can send SNMP traps, while other devices often use syslog as the logging format. Faster deployment and lower maintenance are both benefits of applying agent-less log collection[17].

2.3.8 Communication Platform as a Service

CPaaS stands for Communication Platform as a Service, and is a cloud based communication software that enables organisations to integrate real-time communications[37]. The main use for this is to integrate an organisation's already established applications with communication capabilities through APIs. By doing so, they can limit the amount of resources needed in order to develop their own communication infrastructure. The CPaaS market has now evolved to also using omnichannels, which provide the customer with a seamless and consistent communication experience across platforms. This is done by integrating and synchronising the different communication channels into one solution. Thereby, the CPaaS is used as a middleware to allow communication channels from different vendors to operate as one in the eyes of the users[18].

This is a crucial part of the CSIRT. Without proper communication channels the efforts of the CSIRT would be useless, as the CSIRT needs the capability to communicate with multiple constituents. However, these constituents may use different communication platforms. It is therefore essential that the CSIRT has a way of streamlining their communications across multiple platforms.

2.3.9 Configuration Management Database

A Configuration Management Database (CMDB) is a way for organisations to get an overview of hardware and software used in their infrastructure. The items in a CMDB are called Configuration Items (CI). A CMDB will store relationships and dependencies between these CIs, while also tracking configuration changes. CMDB is a crucial component for establishing a secure environment. As an organisation's infrastructure expands, it becomes increasingly challenging to oversee the hardware and software used. This can pose a significant security risk, as it may result in insufficient updates and misconfigurations. Relationships between CIs are also a pivotal element to track as it becomes easier to comprehend the potential impacts of a hardware or service failure[38].

[37] See: `https://www.techtarget.com/searchunifiedcommunications/definition/Communications-platform-as-a-service-CPaaS`, visited 16.04.2023

[38] See: `https://www.techtarget.com/searchdatacenter/definition/configuration-management-database`, visited 03.05.2023

2.4 MITRE ATT&CK

The MITRE ATT&CK framework is a knowledge hub based on real world observations on known methods an adversary might use when compromising a system[39]. ATT&CK stands for adversarial tactics, techniques, and common knowledge and was created in 2013 by researchers emulating the behaviour of both the adversary and defender[40].

MITRE ATT&CK offers several valuable use cases for CSIRTs. One application is adversary emulation, where the framework is utilised to evaluate an organisation's defence capabilities by simulating attacks that employ the tactics, techniques, and procedures (TTPs) of known adversary groups[19]. This also makes it an excellent component for threat hunting as ATT&CK provides information about most frequently used TTPs, and will aid the CSIRT in pinpointing which group orchestrated an attack[41]. Another potential application for CSIRTs is using ATT&CK proactively to identify security vulnerabilities in infrastructures, by scanning it for potential weak points using the methods outlined in ATT&CK[19].

The use of the MITRE ATT&CK framework can also enhance other platforms. Most SIEMs have integrated the framework into their solutions. For example, IBM has integrated it with their AI called Watson to keep it updated on the latest attack methods[42]. Microsoft has incorporated the framework into their SIEM, Microsoft Sentinel, enabling organisations to visualise their infrastructure's security coverage and identify areas that require improvements[20].

2.5 Human Aspects of CSIRTs

A CSIRT operates a vast number of solutions and resources with the purpose of delivering a specialised service to its constituents. These solutions rely on the competencies and skills of the employees of the CSIRT. SIM3 is a CSIRT maturity model that is widely used and has been adapted by agencies such as ENISA[21]. Additional adaptation have been made by organisations such as GFCE (Global Forum on Cyber Expertise) that further explore the model[22]. While the main purpose of the model is to improve the capabilities of working CSIRTs, it can give a good indication of the human aspects based on the parameters it evaluates. The human parameters emphasised in the SIM3 model are:

- Code of conduct
- Personnel resilience
- Skill set

[39] See: `https://attack.mitre.org/`

[40] See: `https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html`, visited 28.04.2023

[41] See: `https://www.vmware.com/topics/glossary/content/mitre-attack.html`, visited 28.04.2023

[42] See: `https://www.zdnet.com/article/ibm-qradar-advisor-with-watson-boosted-with-mitre-framework/`, visited 29.04.2023

- Training[43]
- Networking

The code of conduct parameters are related to rules and behaviours of a CSIRT. A CSIRT must define a clear set of guidelines on how the staff should act in given situations, both in professional and private settings[22]. This is important as the members of a CSIRT often handle sensitive information related to its constituents, and mishandling that kind of information will lead to losing trust and credibility.

Personnel resilience on the other hand relates to a CSIRT's commitment to provide continuous services, by maintaining a dedicated and adequately staffed team available 24/7. In the adaptation from GFCE, the focus of this parameter is on the ability to keep staff for operational use in cases of illness, holidays, personnel exiting, etc.[22]. While this is most important for the overall function of the CSIRT, it is also important to understand the factors that can cause staff shortages. The working environment can be unpredictable and include high workloads. As threats and incidents increase, there is a significantly higher risk of staff suffering from stress and burnout[24]. Therefore, a CSIRT must also find solutions that can mitigate these issues.

Furthermore, a CSIRT should provide a clear description of the skill set needed in all its roles to provide its services. These should at a minimum include both technical and personal skills[25]. The technical skills being knowledge and experience, including the understanding of both hardware and software solutions as well as incident recognition, analysis, and handling. Personal skills are harder to define, but can be abilities such as communication, teamwork, problem solving, time management, etc. Both personal and technical skills are required to ensure effective and timely incident response from a CSIRT. The FIRST CSIRT Services Roles and Competencies Framework gives a complete look at all roles and skills needed in a CSIRT in correlation with the functions of the FIRST CSIRT Services Framework[26]. The framework is an adaptation of the NIST 800-181 NICE framework and has been reconfigured to suite FIRST[27]. The different roles are described by general tasks, associated functions, generic competencies and role-specific competencies. The generic competencies are personal skills and role-specific competencies are technical skills. To ensure that all staff are properly equipped to handle security incidents and fulfil their responsibilities, a CSIRT must facilitate training processes. These processes include further developing the staff's current skill sets to keep them updated on components, techniques, and procedures. The aim of the training is to improve both technical and personal skills. A report from 2017 showcases that CSIRT staff often had gaps in personal skills that needed additional training[28]. To get the best coverage, the process should include both internal and external training. The internal training will be reliant on establishing mentor programs which require experienced staff with good teaching capabilities[22].

[43]Training refers to the three training-related parameters: internal training, external technical training, and (external) communication training[23].

External training refers to knowledge that is not available within the CSIRT. This can include staff attending courses and acquiring certifications from other cyber security organisations.

The last human aspect emphasised in the SIM3 model is external networking. The parameter refers to the practice of collaborating with other organisations and parties outside of the CSIRT itself. This involves gaining and maintaining relationships with entities such as other CSIRTs, law enforcement, research institutions, etc. By creating a broader network, the CSIRT can get additional assistance during security incidents, as well as stay informed on emerging threats and trends[29]. It would therefore be beneficial for a CSIRT to send staff to industry conferences and attend seminars/webinars to facilitate this.

Chapter 3

Methodology

This chapter will provide a description of the methods used throughout the research process, including a detailed explanation of how the research was conducted, choice of framework, and data collection and analysis.

3.1 Literature Study

Given the limited prior knowledge on the subject matter, the most appropriate method of research was a literature study. The literature study required extensive research, which not only was required for the task, but also for the researchers to gain valuable knowledge on the subject. Therefore, a comprehensive review of relevant existing research and publications was conducted. Figure 3.1 demonstrates the process of the method.

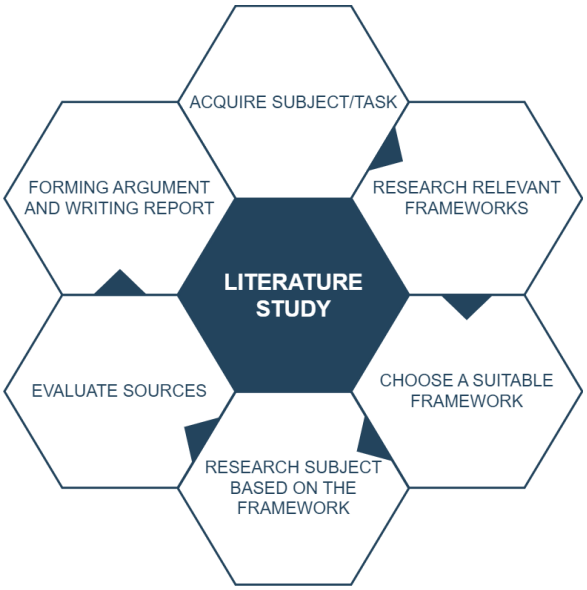


Figure 3.1: Process of literature study (created in diagrams.net)

After acquiring the task, the initial step was to conduct research on frameworks that were relevant to the subject matter, specifically, frameworks that were focused on incident response teams. In doing so, the team ensured to select an appropriate framework for the research purposes, as they were designed for CSIRT operations. Followed by the choice of framework, began the main research objective, which was to comprehensively and systematically conduct research on the components involved in establishing a CSIRT environment. In this part of the process, it was important that the research conducted was in line with the chosen framework. This meant that any discovered solutions had to be supported by the arguments of the framework, in this case the service areas and functions of the FIRST CSIRT Services Framework. Before forming any arguments and writing the report, the sources found through research needed to be evaluated. As already mentioned, one of the criteria was that they had to support the framework. However, other than relevancy to the subject, the sources needed to be credible. It was essential to use sources that were well known for their credibility and accuracy in the cyber security field. Sources will be further discussed in Section 3.5.

3.2 Choice of Framework

To select a specific framework for the thesis, research needed to be conducted on the different frameworks that were available. Early in the process the researchers had been given the FIRST CSIRT Services Framework version 1.1 from the task giver[1]. This facilitated a better understanding of the expectations and requirements of a CSIRT, which made it comprehensible to study other frameworks and compare them in order to find the most suitable one for this thesis. One of the criteria that were set for the framework was that it had to be publicly available. Through online searches and articles the researchers found several different frameworks to potentially base the research on. This included the:

- *ISO/IEC 27035-1:2016*[30]
- *Good Practice Guide for Incident Management*[31]
- *Handbook for Computer Security Incident Response Teams (CSIRTs)*[5]
- *NIST 800-61: Computer Security Incident Handling Guide*[32]
- *FIRST CSIRT Services Framework version 2.1.0*[2]

Collecting all these frameworks made it possible to review and compare them. In the initial search for frameworks, a rough review of each one found was conducted. These reviews were used as a basis on how to evaluate the frameworks further.

In order to evaluate the selected frameworks, a list of different criteria that each had to comply with was created. This was to ensure an effective review of each framework, as well as eliminate any that were not relevant to the task. The criteria were as follows:

[1] https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v1.1.pdf

- **Age of the framework:** The framework should not be more than 10 years old.
- **Capabilities and features:** The framework should have a wide array of features that clearly enhances the CSIRT's capabilities.
- **Ease of use:** The framework should be easy to comprehend without prior knowledge of a CSIRT's functions.
- **Popularity:** The framework should have an already established user base through industry adoption.

The frameworks were evaluated based on the requirements of the task. The focus was therefore limited to frameworks that had been updated in the last ten years. This could have some leeway if the framework scored high in the other criteria. The age limit's goal was to ensure an up-to-date framework based on current technologies and threat assessments. A more recent framework may have more relevant features that cater to the latest trends in CSIRTs. This was important as the current landscape in cyber security is constantly evolving and the task required a framework that was created with this in mind. The age limit was beneficial, as a lack of revisions could indicate a lack of support for the framework from the developers. It can also be a sign of discontinued development on the framework altogether.

Furthermore, the choice of framework had to have a wide range of features and capabilities to properly address the CSIRT's needs. Since there are many different activities a CSIRT must perform, the framework needed to work as a comprehensive guide to incident response as well. An important factor to this was the frameworks ability to translate its own content into solutions available on the current market. This would make it easier to select components for the CSIRT and ensure that the goal of task was met.

Another important factor was the frameworks ease of use. The framework should have a good structure that was easy to navigate and required minimum training to be used effectively. The parties that would benefit from the findings in this report may possess varying knowledge and proficiency on the functions of a CSIRT, which required the framework to be intuitive and user friendly. This involved how work processes and activities were explained in the framework, as well as how it was structured. The structure needed to have defined categories that were intuitive to understand.

Lastly, the popularity of the framework was considered. The popularity would be a good indicator on how effective the framework is in practice. A higher user base would indicate a framework that is well established and tested. This criteria would be used if the ultimate choice was between two or more frameworks, then the most popular would be chosen.

After conducting a thorough comparison among various frameworks, the decision was made to proceed with the FIRST framework. This choice was made as it met all of the set criteria, as shown in Table 3.1. It was the most recently updated framework, which ensured it to be up to date on the latest trends re-

grading CSIRTs[2]. Additionally, categorisation through service areas, supported by underlying services and functions, made it a comprehensive framework while still maintaining an ease of use and understanding.

Table 3.1: Comparison of the various frameworks

Name	Age	Capabilities and features	Ease of use	Popularity
ISO/IEC 27035-1:2016				
Good Practice Guide for Incident Management				
Handbook for Computer Security Incident Repsonse Teams (CSIRTs)				
NIST 800-61: Computer Security Incident Handling Guide				
FIRST CSIRT Framework version 2.1.0				

In Table 3.1, the colours represent the performance of each framework in regard to the set criteria. Green is used to indicate good performance, yellow is used to indicate moderate performance, and red is used to indicate poor performance. *ISO/IEC 27035-1:2016* was a good contender, but was ultimately disregarded as it was reliant on other ISO standards, which made it complicated to use. The *ENISA Good Practice Guide* seemed to have a smaller scope related to components and had a greater focus on workflows and processes, which resulted in a lack of capabilities for the purpose of the task. While *Handbook for CSIRTs* was one of the more popular in regard to citations, it was too old and lacked capabilities for today's threat landscape. Lastly, the *NIST 800-61* was deemed challenging to use, as the structure and layout of the framework made it less intuitive to navigate.

[2]This decision was made before the 13th of February 2023, before the new and updated ISO/IEC 27035-1:2023 was published[33].

3.3 Data Collection

Data collection was an integral part of the research. A CSIRT consists of a wide range of components of hardware, software, and processes to function effectively. This required sources that were not only valuable in increasing the researchers' knowledge in the field, but also essential as a foundation for the thesis.

3.3.1 Data Collection Instruments

The main data collection instruments ended up being the Google search engine, Google Scholar[3], Google's search engine for academic literature, and Oria[4], NTNU's library database. In addition to these, the task giver was a valuable resource in providing relevant sources specific to the problem area.

Examples of different search queries used in the research process:

SQ1: "computer security incident response team"
SQ2: ("csirt" OR "cert" OR "soc") AND ("tools" OR "components" OR "technical solutions")
SQ3: ("information" AND "security" AND ("event" OR "incident") AND "management") AND ("tools" OR "components" OR "technical solutions")
SQ4: ("incident" OR "vulnerability" AND "management") AND ("tools" OR "components" OR "technical solutions")

The different search queries were used in all the data collection instruments, which provided sources for different needs. For example, the Google search engine was valuable in providing sources relevant to specific products, while Google Scholar and Oria were useful in finding technical and academic sources. The process for determining relevant and optimal sources will be further explained in Section 3.5.

3.3.2 National Cyber Security Center (NCSC) – Expert Interview

The researchers had the pleasure of visiting the National Cyber Security Center (NCSC) in Oslo to interview an expert. NCSC serves as a platform for both national and international cooperation in the areas of detection, management, analysis, and advisory services pertaining to digital security. Comprising partners from the business sector, academia, defence, and the public sector, the centre actively engages in collaborative efforts to foster a stronger and more secure digital landscape in Norway[5]. NCSC can therefore be viewed as Norway's national CSIRT.

The interview provided the researchers with valuable insights into CSIRT operations, especially the Norwegian SRM solution. Naturally, a considerable amount

[3] https://scholar.google.com/

[4] https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/search?vid=NTNU_UB

[5] See: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

of information regarding specifics of NCSC's operations and components are confidential. However, the information that was gathered, as well as the experience, was valuable to the team. Notes from the interview can be found in Appendix E.

3.4 Sources

Since good sources are imperative for a good result, a method to evaluate sources in order to determine which ones were acceptable in the research, was needed. To do so, a method known as the CRAAP test was used. CRAAP stands for currency, relevance, authority, accuracy and purpose, and is a way one can test different sources to objectively determine their quality[34].

Figure 3.2: Process of evaluating sources (created in diagrams.net)

Currency is the first step in evaluating a source and it is focused on when a specific piece of information was written, as well as if it has been revised. This is an especially important variable when it comes to cyber security. Technology is in constant development and threat actors regularly find new ways to compromise

systems. Therefore, it was crucial that the sources, and especially the main framework, were up to date. The researchers always sought to use the latest versions of information, and if it was older than 5 years, it would have to justify its age in other ways. For instance, governmental documents on a decision or an important stride in sectoral CSIRTs are examples of justifiable information.

Relevance is about how suitable the information is to the specific topic and problem area. What needed to be considered, other than direct correlation, was also if the level of the information was sophisticated enough to be used in the research.

Authority is an important part of source evaluation and focuses on who authored the given piece of information. An author could be a person, a group of people or an organisation. It was particularly important to be critical to information that was from organisations. The reason being that the research conducted was on a wide range of tools, often from the provider's own documentation. In the case an author was a person or group, looking into their credentials and/or affiliations was a common practice.

Accuracy is strongly related to authority, as reliability and trustworthiness of information is often linked to who wrote the information. However, rather than who, accuracy focuses on where. In this case, it was imperative that the information used was linked to reputable and respected sources in the cyber security field.

Purpose was also a part of the evaluation process that heavily required critical thinking. It focuses on why the information exists. It could for example be to educate or to sell. When researching tools from different providers, it was crucial to keep this in mind, as their main objective was to sell their product.

The CRAAP test was a valuable tool in order to evaluate sources, as the task required a substantial amount of research. Having a method to objectively test sources based on the five mentioned criteria made the process easier, while at the same time assuring the integrity of the research.

3.4.1 Important Sources

Two eminent sources, Gartner and Forrester, warrant special acknowledgement for their pivotal role in identifying relevant components and providers. These reputable entities proved crucial in the decision-making process when selecting components.

Gartner

Gartner was founded in 1979 and is an IT research and consultancy firm. Gartner offers a wide range of services aimed at assisting organisations in making informed decisions regarding IT. One of these services is Gartner's Magic Quadrant. The Magic Quadrant is a research paper on the position and progress of

a company's product in a specific technology, such as SIEM[6]. The report extensively relies on Gartner's Magic Quadrants as a trusted and respected source when selecting specific tools. Gartner's Magic Quadrants hold significant credibility in the industry and several companies would showcase their performance in these evaluations on their respective websites if they scored highly.

Forrester

Forrester exhibits many similarities to Gartner, being a prominent player in the field of research and consulting. Forrester was established in 1983 and around 46% of the Fortune 500 companies are their clients[7]. Similar to Gartner's Magic Quadrant, Forrester publishes its own evaluation framework called the Forrester Wave, which assists organisations in selecting the optimal solutions within a given technology. To maintain objectivity, Forrester declines client engagement during the creation of the Forrester Wave and follows a publicly available methodology[8]. Companies doing well in the Forrester Wave will also usually mention this on their websites.

[6]See: https://www.techtarget.com/whatis/definition/Gartner
[7]See: https://www.forrester.com/about-us/fact-sheet/
[8]See: https://www.forrester.com/policies/forrester-wave-methodology/

Chapter 4

The FIRST Framework

As mentioned in Section 1.2.4, the FIRST CSIRT Services Framework is divided into separate service areas. This chapter will focus on these respective services areas, and the services these contain, in order to give the reader a greater overview of the framework. Having a better understanding of the framework will be advantageous when we discuss our solution and proposed components to establish a CSIRT environment. Figure 4.1 demonstrates how the framework is made up of service areas with their own internal services, while Figure 4.2 demonstrates the overall structure of each service area. The majority of information provided in this chapter is derived from the framework.

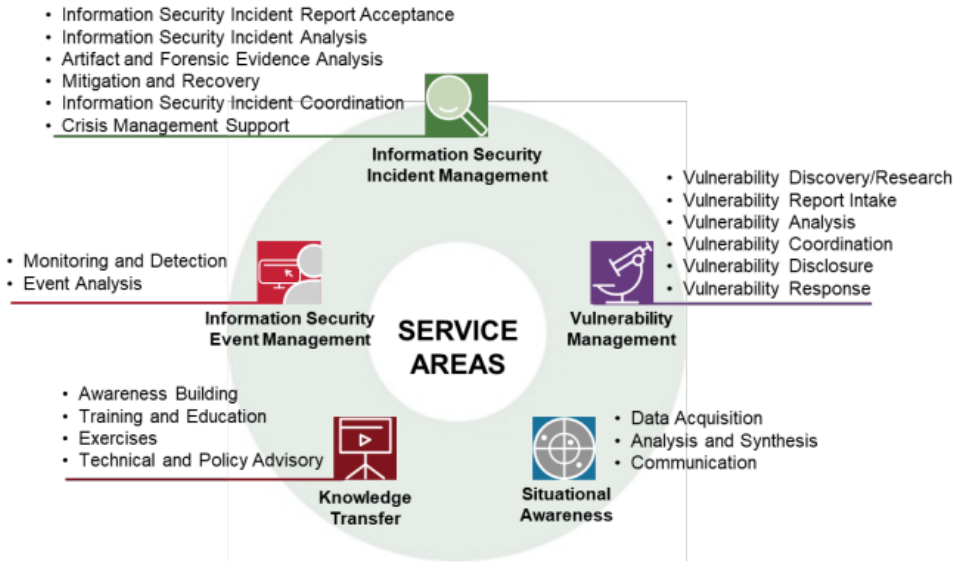


Figure 4.1: Service Areas and Services[2]

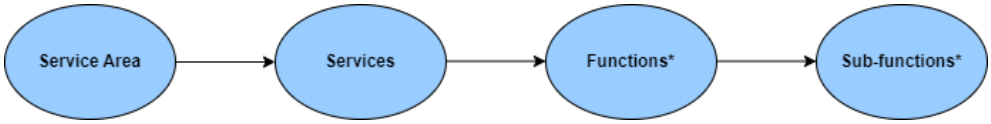


Figure 4.2: Structure of the FIRST Framework (created in diagrams.net)
** Functions and sub-functions will not be covered in this chapter, see Appendix G for relevant functions for each service area.*

4.1 Service Area 1: Information Security Event Management

Information Security Event Management has the objective of detecting information security incidents by analysing and correlating security events from various data sources, including contextual information. This is an especially important service area, as all other service areas depend on the information and analysis deriving from event management. For example, event management is a crucial part of incident management (Service Area 2), as it depends on qualified and accurate information to perform the necessary mitigations and actions to potential security incidents.

4.1.1 Services

Information Security Event Management consists of two services: Monitoring and Detection, and Event Analysis. Both services, with their respective functions within, play a vital part in an effective approach to event management in a CSIRT.

Monitoring and Detection

The purpose of this service involves the implementation of automated information security event sources and continuous processing of contextual data to identify any signs of security incidents. This can be done by the collection of data gathered from a SIEM, as explained in Section 2.5.1. Therefore, it is vital to have the necessary components in place to gather this information, as well as adequate management of the components and collected data, to ensure an effective approach to event management.

Event Analysis

Event analysis involves triaging of potential information security incidents where the objective is to assign them levels of importance or urgency. This determines the order in which the incidents will be further investigated[1]. Detection of possible se-

[1]See: `https://learn.microsoft.com/en-us/microsoft-365/security/defender/first-incident-analyze?view=o365-worldwide`, visited 05.04.2023

curity incidents is done through the implementation of the previously mentioned service, and triaging can be completed both manually by a security analyst and through automation by a SIEM (2.5.1).

Through effective analysis a CSIRT can group related security incidents and determine true or false positives. Grouping security incidents is done by considering security incidents related to the same assets or identities as one incident, instead of separately. By doing so, the duplication of the same incident is avoided in an effort to streamline incident management. As mentioned, triaging is an essential part of event analysis, and it is by triaging one can determine whether a potential security incident is a true or false positive.

4.2 Service Area 2: Information Security Incident Management

The aim of this service area is to offer assistance to constituents during attacks or incidents. In order to do so, the CSIRT must have the necessary tools and competencies to manage such scenarios. It is therefore crucial that the CSIRT has the ability to use the collected data and analyse it accordingly. This includes activities such as accepting incident reports from constituents as well as root cause analysis and artefact forensics. As a result, the CSIRT can make recommendations to help mitigate the current incident and give advice on recovery plans.

4.2.1 Services

Information Security Incident Management consists of six services. Each of the services support a different aspect of the service area, which a CSIRT can utilise to support its constituents.

Information security incident report acceptance

The CSIRT has to be able to receive and process incident reports from multiple sources, either from its own constituents, services from other service areas or external entities. These reports can either be received automatically through Information Security Event Management or manually through reporting mechanisms. Since reports can derive from multiple sources and formats, it is imperative that the CSIRT is prepared to handle them.

Information security incidents analysis

This service involves understanding the information security incident. It involves a detailed analysis that is set to determine the root cause and assess the impact of the incident. The analysis is necessary to characterise the incident and determine the scope, affected entities, tools and vulnerabilities used by the attacker, as well as the timeline of the event.

Artefact and forensic evidence analysis

Digital artefact analysis aims to understand how the artefacts of an information security incident were utilised in an attack. The analysis consists of identifying the capabilities and intent of an artefact. This should include how the artefact initially infected the system, how it spread throughout the system, as well as its discovery and eliminations. Artefact forensics requires high level expertise as well as a dedicated analysis environment. All associated artefacts must be preserved without modification as they can be used as evidence in criminal cases. The information gathered on the artefacts could be essential to share with constituents and third parties, in order to either raise awareness or establish mitigation strategies.

Mitigation and recovery

This service aims to mitigate the information security incident to the best ability and minimize overall damages. This is achieved through developing response plans and implementing temporary ad-hoc measures. The ad-hoc measures may be set in place before a response plan is established to ensure that the incident is as contained as possible. The outcome of this service includes swift mitigation of incidents and improvement of the cyber security posture, as well as the restoration of impacted services.

Information security incident coordination

The purpose of this service is to ensure optimal communication and coordination among all entities involved in responding to an information security incident. It involves establishing suitable escalation and reporting functions, updating newfound information, and providing channels for stakeholders to submit questions and report issues. The outcome is a successful and well-coordinated response to the incident.

The CSIRT should maintain channels of communication with both internal and external stakeholders, providing updates on the remediation status and engaging with other CSIRTs and communities for recommendations or technical support. Overall, the aim is to keep the information flow moving and track activities to ensure the response plan is carried out effectively and efficiently.

Crisis management support

The purpose of this service is to provide support and expertise to constituents. CSIRTs can prove to be a crucial resource in managing such incidents, thanks to their experience, established services, and networks of contact points. As a result, the CSIRT can assist crisis management teams in addressing the cyber security aspects of ongoing crises, aiding in tackling the situation more effectively. In addition, the CSIRT's communication resources can be used to reach out to other entities and external parties to ask for specific support actions or assistance.

4.3 Service Area 3: Vulnerability Management

The primary objective of vulnerability management is to discover, analyse, and address new or reported security vulnerabilities in information systems. To do so, the service area includes several services to support the implementation of a comprehensive vulnerability management strategy.

4.3.1 Services

The Vulnerability Management service area consists of six services, all of which play a critical role in improving an organisation's security posture and reducing risk of exploitation when implemented by a CSIRT.

Vulnerability discovery / research

In order to increase the discovery of new vulnerabilities, this service aims to find previously unknown vulnerabilities through activities from other service areas, as well as by the vulnerability management team of a CSIRT. This is the first stage in a further vulnerability management life cycle. Vulnerabilities do not necessarily need to be discovered internally, they can also be found through public sources, such as news and websites, as well seeking out potential vulnerabilities through deliberate research.

Vulnerability report intake

A key aspect of a CSIRT's function is the intake of reports from constituents and third parties, including reports related to vulnerability information. The aim of vulnerability report intake is to streamline the reporting process for these parties by providing a structured mechanism, process, guidelines, and reporting infrastructure. Thereby, a CSIRT can ensure that incoming reports are received and processed in a professional and consistent manner.

Vulnerability analysis

Following the discovery of a vulnerability, either reported from constituents or third parties, or from activities by the CSIRT, the next step is seeking to understand it. Through analysis, knowledge of key details on the vulnerability is increased. This gained understanding can benefit the CSIRT in preventing or minimising the exploitation of the vulnerability.

Vulnerability coordination

The vulnerability coordination service involves exchanging information to all parties associated with the coordinated vulnerability disclosure. The different parties associated with this service can be the vendors and developers as well as researchers

and other CSIRTs. The sharing of information plays a critical part in vulnerability management. It used to find remediation and mitigations more effectively for known vulnerabilities, and therefore decrease the risks of incidents occurring.

Vulnerability disclosure

The purpose of this service is to use the knowledge gathered from the previous services and inform the constituents directly of known vulnerabilities. This will facilitate the constituent in taking the necessary steps to prevent, detect, and resolve them. This requires established communication channels in order to get the information to the constituents effectively and timely. The communications channels vary such as website, email, SMS, vulnerability databases and other media.

Vulnerability response

The Vulnerability Response service is designed to actively respond to known vulnerabilities by detecting and mitigating them. This includes actions such as purposefully scanning constituents' systems for vulnerabilities and following up on eventual detected vulnerabilities. The purpose of this service is to determine if a disclosed vulnerability exists in scanned systems. While this service is a part of the FIRST CSIRT Services Framework, the related functions of this service are usually carried out by other, more specialised groups, such as a SOC or the system owners.

4.4 Service Area 4: Situational Awareness

The situational awareness service area focuses on a CSIRTs ability to gather relevant information in and around its area of responsibility. As a result, the CSIRT must actively monitor various news and information channels, such as TIPs (2.5.3), to identify any developments that may have a potential impact on the operations of a constituent.

Information collected in the Situational Awareness service area will also be utilised to improve the capabilities and effectiveness of other service areas such as Information Security Event Management, Information Security Incident Management, and Knowledge Transfer. In addition, data collected from these service areas will be utilised in a reciprocal manner to disseminate relevant information back to the constituents in a timely and effective manner.

4.4.1 Services

Situational awareness consists of three services. Each service promotes the ability to gather, integrate, and communicate relevant information from different sources.

Data acquisition

The aim of this service is to gather data that can enhance the understanding of both internal and external activities that have the potential to impact the security posture of a constituent. To achieve this goal, the CSIRT will initially establish the acceptable conditions under which the constituent and its infrastructure should be operating. This is important to establish the assets associated risks, and its function and role in the infrastructure. The service also outlines ways of identifying and collecting data that can be used for other services in the FIRST framework such as event management, incident management, and knowledge transfer. This data will then need to be normalised and validated.

The outcome of this service is that the CSIRT will have information about the current and expected future status of a constituent's assets and activities, information about external events or trends, and properly formatted information organised for analysis and detection activities.

Analysis and synthesis

The analysis and synthesis service aims to discern the current or future situational states using the data acquired on the assets of a constituent. To ascertain the present situational picture, a CSIRT must undertake a systematic and often directed search for anomaly activities occurring both within and beyond the network confines. The service also outlines that a CSIRT should look for new information after a security incident. This is to limit the damage, prevent future risks, or identify any new vulnerabilities that may have resulted from the incident.

The outcome is an updated situational picture, along with the identification of future changes by leveraging security event data extracted from the constituencies.

Communication

The communication service focuses on providing the constituencies with reliable information in a comprehensible format, with the aim of assisting them in the implementation of recommended actions and infrastructure improvements. The shared knowledge can also be used to create best practices, reports, and training through the Knowledge Transfer service area. Lastly, the CSIRT is required to obtain feedback regarding the effectiveness of its communication and the reports it has distributed to the respective constituencies.

4.5 Service Area 5: Knowledge Transfer

Knowledge transfer refers to the process of sharing information, expertise, and best practices from one entity to another. Knowledge transfer is a critical component of a CSIRT's role in improving cyber security across an organisation. CSIRTs are well-positioned to collect and analyse relevant data, identify emerging threats

and trends, and develop best practices for incident detection, prevention, and response. The knowledge and insights gained from these activities can be shared with stakeholders and constituents, thereby enhancing their overall cyber security posture.

4.5.1 Services

Knowledge transfer consists of four services. Each service promotes the transfer of knowledge and training between a CSIRT and its constituents.

Awareness building

The Awareness Building service is designed to increase the overall security posture of a constituent by educating its members on how to detect, prevent, and recover from incidents. It involves researching and aggregating relevant information from different security channels, such as TIP mentioned in Section 2.5.2. The CSIRT will use the aggregated data to develop reports and awareness materials. The reports developed will also serve the purpose of establishing and maintaining cooperation with experts and organisations (e.g., through TIPs and ISACs).

The ultimate outcome of this service is that the constituent is provided with the necessary awareness on security, operational best practices and trends that may affect its ability to operate securely. It will equip the constituent with the knowledge necessary to identify, prevent, and mitigate threats and malicious activities by providing actionable steps.

Training and education

The Training and Education Service aims to educate the CSIRT's constituencies on security. The service will initially ascertain deficiencies in employees' cyber security knowledge by utilising techniques, such as surveys and discussion forums. The service subsequently devises strategies for creating and disseminating educational materials that effectively address the identified knowledge gaps. Additionally, the service prioritises the fostering of mentor relationships amongst employees.

The outcome is a consistent training and education program that enables the CSIRT's constituencies to appropriately acquire the necessary method, tools, and practices to detect, prevent or respond to threats.

Exercises

This service provides cyber security exercises to assess and improve the effectiveness and efficiency of cyber security services and functions. These exercises are designed to evaluate the adequacy of policies and procedures and assess the readiness of a constituent in responding to potential security incidents. To create realistic and effective exercises, the CSIRT can make use of attack simulation

tools, as well as note-taking and planning tools, to assess whether the exercise proceeded as intended.

The outcome is an improvement in the effectiveness and efficiency of security operations and capabilities, as well as identification of opportunities for further improvements.

Technical and policy advisory

This service provides technical and policy advisory to a CSIRT's constituencies and key stakeholders, as well as placing emphasis on knowledge dissemination among its own staff. The CSIRT will offer technical guidance to enhance the security posture of a constituent's infrastructure, encompassing advice on the appropriate tools and services to be utilised.

The outcome of the service will provide the ability to build the capability, capacity, and maturity of a CSIRT and enhance the security posture of a constituent.

Chapter 5

Proposed Technical Solutions for the CSIRT

This chapter will present the findings of the research, which are the technical solutions required of a CSIRT to support the functions of the FIRST framework. To do so, multiple components are required. These are presented in this chapter, along with their technical abilities, which functions they support and why they would be a sensible solution for the CSIRT. Appendix F is highly relevant material in regards to this chapter in order to fully comprehend the functions each component of the CSIRT environment supports. It is a detailed table that showcases the relevant functions to the corresponding components, which will provide additional information that is otherwise not covered.

5.1 Visualisation of Data Collection

Figure 5.1 demonstrates how the CSIRT will perform its data collection. Data derives from external networks, where sensors and a variety of data collection components are deployed. From there, the necessary data such as logs, network traffic and application reports are forwarded to the CSIRT's database. As data is collected from constituents and stored inside the CSIRT's internal network, the SIEM is prepared to receive and process that data with the help of its built-in functions. In the following sections, we will provide a detailed account of the proposed components for the CSIRT with respect to the components referenced in the figure.

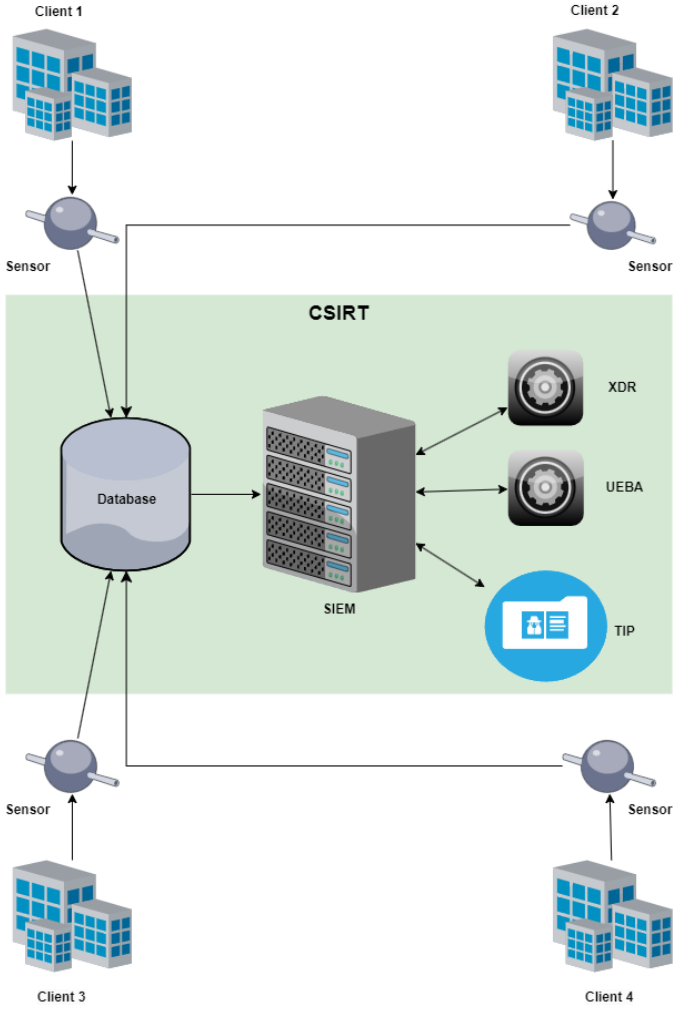


Figure 5.1: Example of data collection architecture (created in diagrams.net)

5.2 SIEM

A SIEM is at the heart of a CSIRT's operations and therefore naturally covers a considerable part of the FIRST framework's functions (see Appendix F). According to Gartner, Microsoft is a Leader in the SIEM market[35]. A Leader satisfies both the market's and the customer's requirements, while showing evidence of superior vision and execution for future requirements . A Leader is also a vendor that has been one of the most successful in the market. Success is based on the product itself, as well as market share and revenue growth. Based on Gartner's Magic Quadrant for Security Information and Event Management, Microsoft Sentinel was determined to be the optimal SIEM solution for Digdir's CSIRT needs. Figure 5.2 visualises Gartner's Magic Quadrant, showing Microsoft as a Leader, as well as where other competitors stand.

Figure 5.2: Magic Quadrant for Security Information and Event Management[35]

5.2.1 Microsoft Sentinel

Microsoft Sentinel is a solution that satisfies multiple functions of the FIRST framework including functions in Information Security Event Management, Information Security Incident Management, Vulnerability Management, and Situational

Awareness (see Appendix F). Sentinel is a cloud native SIEM solution that is built on the Micosoft Azure cloud platform[1]. As a SaaS service, Sentinel leverages key advantages, such as scalability and cost-effectiveness. Moreover, given Digdir's ambition to migrate several of their platforms to Microsoft Azure clouds, strengthens Microsoft Sentinel as their CSIRT SIEM solution[2]. The reason being that Sentinel comes with a wide range of out-of-the box data connectors that are easily integrated with Microsoft's native solutions[36]. Microsoft 365 Defender is an example of a data connector that can be integrated with data sources such as Office 365 and Azure Active Directory, allowing for seamless data collection[37].

Once the data is collected, Microsoft Sentinel uses a vast number of technologies and techniques in order to process the data collected. One of these is the UEBA engine (2.5.3). Figure 5.1 depicts the relationship between the SIEM and UEBA. The engine builds a baseline behaviour profile for entities in a constituency, based on users, hosts, IP-addresses and applications[3]. This profile can then be used to determine abnormal activity and if a user has been compromised.

Although Sentinel is highly integrated with Microsoft's ecosystem, it can still be used with third-party sources, including syslog and through REST API connections[37]. As explained in Section 2.5.1 and 2.5.6, a SIEM is entirely dependent on a diverse set of data types to perform its functions, making third-party integrations essential. The wide range of data sources a SIEM will ingest derive from sensors stationed at constituents' networks. The different sources and types of data will therefore be discussed in more detail in Section 5.4. Furthermore, the MITRE ATT&CK framework (2.6) is highly integrated in Sentinel, which allows for sophisticated analysis and threat hunting by the SIEM[20].

5.2.2 Microsoft 365 Defender (XDR)

As described in Section 2.5.1, the terms SIEM and XDR are often used interchangeably. The solution presented in Figure 5.1 shows a deployment that uses an integrated XDR and SIEM solution. The SIEM and XDR's value relies on its ability to ingest and process the received data from its sources. While the SIEM uses multiple sources, such as information from external parties and TIPs, the XDR provides a more direct approach to detection of endpoints and networks. When XDR is integrated with a SIEM solution, it enhances the depth and contextual understanding of security events and incidents. This is because XDR solutions typically integrate data from sources such as endpoints, network traffic, cloud services, and other security products. By combining this data with the data collected by the SIEM

[1] See: https://learn.microsoft.com/en-us/azure/sentinel/overview, visited 06.05.2023

[2] From meetings with the task giver as well as several sources indicate this. See: https://www.digdir.no/digdir/nytt-direktorat-pa-294-dagar-og-ny-it-infrastruktur-pa-105/1780 and https://www.digdir.no/digitale-felleslosninger/altinns-nye-skyplattform-i-produksjon/1590 and https://www.digi.no/tumstudio/skytjenester/annonse-slik-skal-digdirs-skyovergang-loses/517578, visited 08.05.2023

[3] See: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics, visited 06.05.2023

solution, the CSIRT can get a more comprehensive understanding of the entire security landscape and identify potential threats swiftly and accurately. In this solution the XDR is supposed to support the SIEM with its data collections. By doing so, it is supporting several of the same services and functions as the SIEM according to the FIRST framework (see Appendix F).

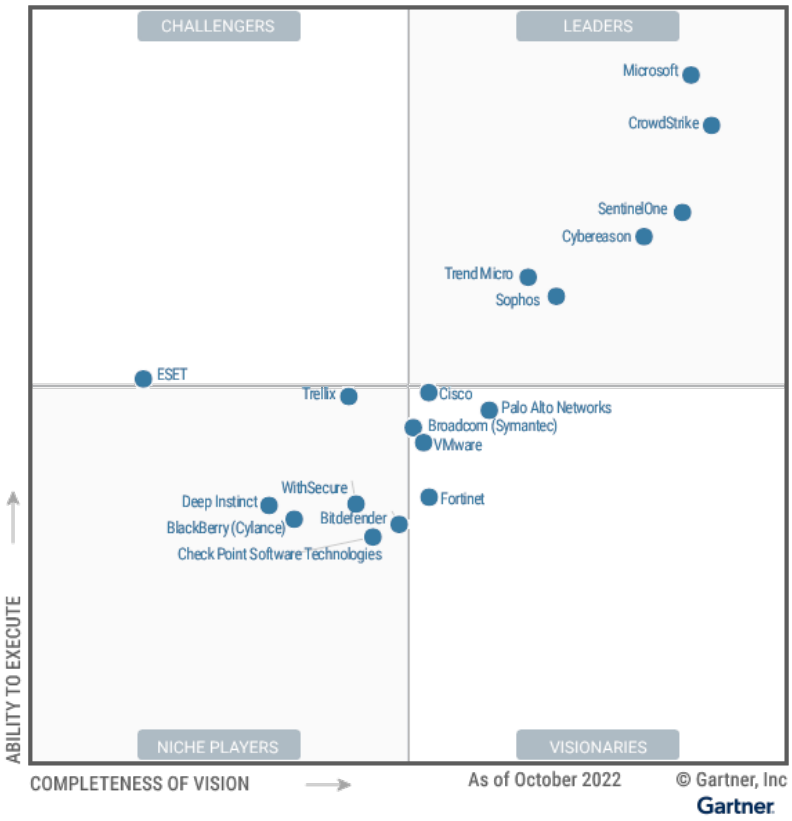


Figure 5.3: Magic Quadrant for Endpoint Protection Platforms[38]

Microsoft 365 Defender is Microsoft's answer to the demand for an XDR solution. Microsoft is regarded as a leader in the Gartner Magic Quadrant for Endpoint Protection Platforms, and scores highest in its ability to execute, as shown in Figure 5.3. The ability to execute refers to a company's ability to deliver products and services that meet the customers needs and expectations[39]. Microsoft's scoring means that it is regarded as a strong figure in the industry and has a good track record of delivering high-quality products and services. This serves as a reliable indicator of the product's performance capabilities.

In order for Microsoft 365 Defender to perform at its optimal level, it is recommended that it coordinates with different services such as[4]:

- Microsoft Defender for Endpoint

[4]See: `https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide`, visited 07.05.2023

- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Data Loss Prevention
- App Governance

Microsoft Defender for Endpoint is a core component of Microsoft 365 Defender. It contains various features that increase the XDR's ability to detect and respond to threats. Microsoft offers this service through various security plans, with the ability to extend it with the defender vulnerability management add-on. The features included give a comprehensive solution for endpoint detection and response by the XDR. This includes abilities such as discovering devices and endpoints in a system, detection and response, and threat analytics[5].

Microsoft Defender for Office 365 is an email filtration service that support the XDR in detecting abnormalities in email-based threats. This includes threats such as spam, phishing, malware, spoof intelligence and impersonations. It analyses email content, attachments, sender reputation and behavior, and employs heuristics to detect suspicious messages[6]. Additionally, it includes a sandbox environment for opening attachments and running URLs to identify and isolate potentially malicious code, which can then be used to investigate them further.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that helps organisations maintain the security of their cloud environment. With this tool, businesses can gain visibility and analytics to detect and prevent cyber threats across various cloud services, both from Microsoft and third-party providers[7]. Using Cloud Discovery technology, the solution is capable of scanning and identifying all cloud assets and applications within a given environment. Moreover, it comes with a pre-built cloud app catalog that ranks applications according to their risk factors[8]. By working in conjunction with App Governance, Microsoft Defender for Cloud Apps offers enhanced oversight over all application activities and potential security threats[9].

These products are important to help the XDR get as much available information as necessary. By integrating these products with Microsoft 365 Defender, the CSIRT can achieve a comprehensive XDR solution that provides extensive visibility and protection across their entire security environment. The integration allows

[5] https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2?view=o365-worldwide#compare-microsoft-endpoint-security-plans-1, visited 07.05.2023

[6] https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide, visited 07.05.2023

[7] https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps, visited 08.05.2023

[8] https://learn.microsoft.com/en-us/defender-cloud-apps/editions-cloud-app-security-aad, visited 08.05.2023

[9] https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-manage-app-governance, visited .05.2023

Microsoft 365 Defender to correlate data from different sources and provide a unified view of security events and incidents, enabling Digdir's CSIRT to detect and respond to threats more rapidly and efficiently. It is important to mention that the main downside of a XDR is its data retention. However, this is remedied by integrating it with the SIEM solution. At the same time the integration may cause some of the related XDR products to become redundant. This is apparent with Microsoft Defender for Identity as it utilises the same capabilities as the Microsoft Sentinel's UEBA engine, as mentioned in Section 5.3.1.

The CSIRT solution presented uses Microsoft 365 Defender based on its wide range of capabilities and findings from Gartner. However, it is important to note that this solution requires specialised competencies and awareness around Microsoft's licensing variations in order to get the desired features.

5.2.3 MISP (TIP)

Threat intelligence is a fundamental part of a CSIRT's ability to aid its constituents in potential security incidents. According to NIST, threat intelligence is any information that can help the CSIRT to identify, assess, monitor, and respond to cyber threats[40]. This highly valuable information can be shared among organisations, for example between CSIRTs, to collectively improve security postures. This can be done through Threat Intelligence Platforms, such as MISP. MISP stands for Malware Information Sharing Platform and is an open-source threat intelligence platform that can collect, store, distribute and share threat intelligence[41]. Sharing of threat intelligence is a process that strengthens multiple functions of the FIRST framework, most notably with respect to Situational Awareness and Knowledge Transfer (see Appendix F).

The justification for endorsing MISP as the CSIRT's TIP is not solely based on its potential to bolster the functions of the FIRST framework, but also derives from its extensive user base and community of threat intelligence sharing contributors. Furthermore, MISP was partly developed and used by the North Atlantic Treaty Organization (NATO)[10]. Being affiliated with NATO is an important factor, as Digdir is an agency of an Allied country.

MISP also has the ability to create "sharing instances" or communities for threat sharing purposes. FIRST has its own such instance, and members of FIRST are able to join to share and store threat intelligence data with other members[11]. In order to become a FIRST member, an organisation would have to be endorsed by at least two other member organisations (see Appendix E). There are several FIRST members in Norway, which makes it likely for Digdir to become a member should they wish to. In that case, FIRST's MISP instance would be a sensible choice of threat sharing community, in addition to Norwegian sectoral-wise CSIRT communities.

As Figure 5.1 demonstrates, MISP and the SIEM (Microsoft Sentinel) share a

[10] See: `https://www.misp-project.org/who/`, visited 10.05.2023

[11] See: `https://www.first.org/global/sigs/information-sharing/misp`, visited 10.05.2023

relation. This means that MISP can be integrated with Microsoft Sentinel, allowing for threat intelligence indicators to be uploaded to Sentinel[12]. Integration is made possible by pyMISP, which is a Python library used to access MISP platforms through their REST API, as well as data connectors through Azure, which will be further explained in the following section[42].

5.3 Sensors

Effective log collection is essential for the successful operation of a CSIRT, and it supports important functions in both Information Security Event Management and Information Security Incident Management (see Appendix F). However, log collection also presents a challenge to CSIRTs, as it takes place across multiple devices within an organisation's infrastructure, and will therefore require diverse collection methods. Another challenge is that the infrastructure is not managed directly by the CSIRT, but by its constituencies, which requires a knowledgeable and capable IT department. This section will explore the data sources available to Microsoft Sentinel, the types of data that can be obtained from different components in a constituent's infrastructure, and the prerequisites for successful data collection. Figure 5.4 demonstrates the entirety of the proposed sensor architecture that would be deployed in a constituent's infrastructure. The components making up this architecture will be further explored in this section. However, before proceeding to this detailed explanation, it is imperative to first clarify the distinct ways Microsoft Sentinel can collect data.

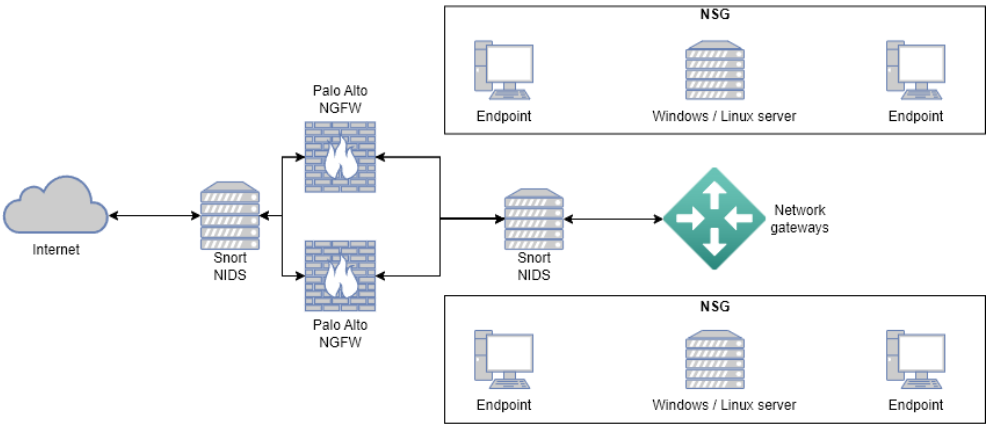


Figure 5.4: Proposed sensor architecture (created in diagrams.net)

[12]See: https://www.misp-project.org/2023/04/03/MISP-Sentinel.html/, visited 10.05.2023

5.3.1 Microsoft Sentinel Data Collection Methods

Microsoft Sentinel can gather data from a variety of sources and in different formats. One way is through the use of agents (2.5.6), such as the Azure Monitor Agent, which can be installed on Windows and Linux machines to collect logs and metrics. The agent sends this data to Sentinel in a standard format, such as JSON or syslog, which can be easily analysed and correlated to detect potential security threats[43].

Another way is through the use of data connectors, which can pull data from third-party sources such as firewalls, intrusion detection systems, and cloud services. These connectors can ingest data in various formats, such as CSV, JSON, or REST API connections, and transform it into a standard format for analysis by Sentinel[37].

5.3.2 Flow Data Collection

Palo Alto Networks' Next-Generation Firewall

The Palo Alto Next-Generation Firewall (NGFW) is a highly respected network security solution that has been recognised as a leader in Gartner's Magic Quadrant for many years, as shown in Figure 5.5. NGFWs are advanced network security solutions that have been designed to address the limitations of traditional firewalls by offering additional security features, such as deep packet inspection and application awareness. This is in contrast with traditional firewalls, which mostly provide packet filtering based on predetermined rules or policies[13]. Other alternatives included Fortinet NGFW and Cisco Firepower, but given Palo Alto's extensive experience in the field, and their track record in Gartner's Magic Quadrant, their solution was deemed optimal for the CSIRT's NGFW solution.

[13] `https://www.intercity.technology/blog/next-generation-firewall-ngfw-vs-traditional-firewall`, visited 09.05.2023

Figure 5.5: Magic Quadrant for Network Firewalls[44]

For optimal security, it is recommended that the constituencies deploy two NGFWs to ensure redundancy, as demonstrated in Figure 5.4. This is essential, as firewalls require regular updating and maintenance. Relying on a single firewall could result in gaps in security and log collection during downtimes. Having two NGFWs in place ensures that the network remains secure and fully operational, even if one of the devices experiences issues.

The Palo Alto NGFW creates a considerable amount of valuable logs that can be forwarded to the CSIRT. According to Palo Alto, some of these logs are[14]:

- Threat reports
- Traffic
- URL filtering
- WildFire Submissions
- Data filtering
- HIP Match
- Correlation event logs
- Tunnel logs

[14]See: `https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/monitor/monitor-logs/log-types`, visited 09.05.2023

- Config logs
- Authentication logs

The NGFW logs offer significant value to a CSIRT. These logs enable the CSIRT to effectively monitor the applications that are being used within a constituency. Furthermore, Palo Alto's NGFW provides threat reports on any potential threat actors that have attempted to penetrate the network. This level of visibility into the network traffic can aid the CSIRT in swiftly detecting and responding to any potential security incidents[45].

In addition to monitoring applications and threats, Palo Alto's Wildfire feature can also monitor the sharing of files, including files that may be malicious in nature. This functionality is particularly valuable for a CSIRT as it enables them to rapidly detect and respond to any potential threats posed by file sharing within the network. It may also prove valuable in the aftermath of an attack, as it could reveal the extent of sensitive information obtained by an attacker. Additionally, the configuration of the firewall is logged by the NGFW, which can be valuable in identifying and investigating insider threats[45]. Microsoft Sentinel has the capability to ingest data from Palo Alto Network's NGFW via a data connector[15].

Snort

Snort is an open-source lightweight packet inspector that can run as either an Intrusion Protection System or Intrusion Detection System (IPS/IDS)[16]. When Snort runs as an IPS, it employs a set of predefined rules to identify and alert the system to the presence of malicious packets. Two methods exist for defining the rules in Snort. One approach involves utilising rule definitions provided by Cisco, which are updated as new rules are developed. The second method is community development, where the rules are defined through the collective efforts of the community. It is possible to simultaneously employ both methods to define the rules in Snort. In IDS mode, Snort will act as a packet sniffer, and will serve to collect traffic data[17]. The data can then be forwarded to Microsoft Sentinel for further analysis and action. Figure 5.4 reveals the placement of multiple Network Intrusion Detection Systems (NIDS, 2.5.6) in the sensor architecture. The NIDSs outside the firewall provides the CSIRT with valuable insight into attempted attacks on the constituency, including the frequency of attempts and the location of the source. Furthermore, the NIDS beyond the firewall will inspect packets that have already been filtered by the firewall. This sensor will provide the CSIRT with information on attacks that managed to get through the firewall and what information an attacker managed to steal as it left the infrastructure. Having both these sensors installed will also facilitate comparison of data and monitoring of the firewall's

[15] See: `https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/palo-alto-networks-firewall`, visited 08.05.2023

[16] `https://www.snort.org/`, visited 07.05.2023

[17] See: `https://linuxsecurity.com/features/network-intrusion-detection-using-snort`, visited 07.05.2023

effectiveness[18] .

For Snort to send logs that Sentinel can interpret, it must be sent as syslog. A custom agent also has to be made in Sentinel as Snort does not have the required data connector[19]. The reason Snort is considered ideal, is because it is lightweight, open-source, community supported and integrates well with Microsoft Sentinel. Several tools were evaluated for the purpose of integrating an IDS with Microsoft Sentinel. Among them were SolarWinds and ManageEngine Log360[20]. However, these tools were deemed sub-optimal due to their inability to integrate seamlessly with Sentinel, as their IDS is part of a larger solution. Furthermore, other IDS solutions evaluated were primarily HIDSs (Host Intrusion Detection System, 2.5.6), or had converted their IDS solution to an IPS, which was not necessary for the specific requirements of Digdir's CSIRT solution.

Azure Network Watcher

It is imperative to monitor the data flow inside a constituent's infrastructure. Network flow data inside the constituent's infrastructure can provide information on the movements of intruders and potentially compromised machines, if an attacker has managed to get inside the network. As described in Section 2.4.2, an attacker will try to compromise as many systems as possible. The implementation of an IDS can greatly assist the CSIRT in identifying and mitigating these attacks, as well as facilitating post-incident recovery efforts[21]. Furthermore, data flow monitoring inside the constituent's infrastructure can facilitate the detection of insider threats, such as malicious employees who may have access to sensitive information. By monitoring the traffic flow between departments, the CSIRT can identify any unusual or suspicious activities and take necessary action to prevent or mitigate any potential damage[22]. Snort could be used for this purpose, however, Microsoft has its own IDS solution called Azure Network Watcher, which monitors network data between network security groups (NSG). NSGs allow you to control inbound and outbound traffic to and from Azure resources, such as virtual machines and subnets. Each NSG contains a set of security rules that specify the type of traffic allowed[23]. This is the optimal approach, due to the seamless integration

[18] See: https://www.informit.com/articles/article.aspx?p=782118, visited 08.05.2023

[19] See: https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference, visited 08.05.2023

[20] See: https://www.solarwinds.com/security-event-manager/use-cases/intrusion-detection-software and https://www.manageengine.com/products/eventlog/ids-ips-monitoring-reporting.html?lhs, visited 06.05.2023

[21] See: https://netacea.com/glossary/network-intrusion-detection-system-nids/, visited 11.05.2023

[22] https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4c7876fe-4fe7-4931-9e80-b420f38200b0&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, visited 12.05.2023

[23] https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview, visited 12.05.2023

with Sentinel.

5.3.3 Endpoint Data Collection

The adoption of Microsoft's proprietary collection methods, specifically Azure Monitor Agent (AMA), is viewed as most favourable solution for endpoint data collection. AMA seamlessly integrates with various Microsoft products, including Microsoft Sentinel, enabling the utilisation of comprehensive functionalities such as UEBA and machine learning capabilities. Endpoints, encompassing virtual machines, computers, and servers, and are effectively monitored and analysed through this selected approach[43].

Additional viable alternatives include tools such as NXlogs and Logstash, which facilitate log filtering prior to their transmission to Microsoft Sentinel[46]. Employing log filtering tools carries both advantages and disadvantages for a CSIRT. On the one hand, it streamlines the logs, retaining only the necessary information, resulting in a reduced volume of logs that necessitates less infrastructure to manage and will reduce the noise created from insignificant logs[24]. On the other hand, the use of filtered logs may result in certain functions becoming unavailable in Microsoft Sentinel[46].

AMA offers a combination of advantageous features from both perspectives. As it is a monitor tool provided by Microsoft it can filter logs without losing functionalities, such as UEBA, in Sentinel[46]. AMA is an agent-based log collection method (2.5.6). However, agent-based log collection may not be feasible in all scenarios. In such cases, the constituent may have to rely on agent-less log collection. Microsoft has an agent-less solution called Windows Event Forwarding that it recommends using during such scenarios. Therefore, the CSIRT might have to use both solutions when collecting endpoint data[46]. AMA collects the following logs from endpoints[43]:

- Event Logs
- Performance logs
- File based logs
- IIS logs

Event logs offer the CSIRT valuable insight into applications running on endpoints as well as events relating to security and system information[25] . Performance logs will monitor and send information on how resources are being used on endpoints, as well as the performance of the operating systems and applications[26]. File-based logs are logs that cannot be easily converted into standard formats such as syslog

[24] `https://nxlog.co/news-and-blog/posts/reduce-data-size-and-cost/`, visited 14.05.2023

[25] `https://www.solarwinds.com/resources/it-glossary/windows-event-log`, visited 14.05.2023

[26] `https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-performance-counters`, visited 13.05.2023

or Windows Event Logs. Consequently, they must be transmitted as text files[27]. Lastly, IIS logs which stands for Internet Information Services, are logs regarding user activities[28].

AMA was created to replace legacy agents such as the Log Analytics Agent. It was released in June 2021 and has therefore less capabilities than the legacy agents, as it is still in development[29]. This is noteworthy since these legacy solutions will have no further support beyond 2024, making AMA a better long-term solution[43].

Sensor Management and Mapping

The vast number of sensors present at each constituent will require updating and managing. One viable solution for addressing this challenge is Microsoft's System Center. System Center has two main components, System Center Configuration Manager (SCCM) and System Center Operations Manager (SCOM)[30]. Another important component of System Center is Service Manager (SCSM).

Accoring to TechTarget, SCCM can be used for Windows management, operating system deployment, software update management and application delivery[31]. Application delivery enables the CSIRT to remotely deploy applications such as AMA, significantly reducing the workload by eliminating the need for manual installation on each endpoint within every constituency. The sensors will also need updates and changes in configuration through their life cycle as circumstances change. SCCM can assist in this matter, as it provides easy remote management of devices and applications.

SCCM plays a pivotal role in the Monitoring and Detection service within the Information Security Event Management service area (see Appendix F). Other alternatives to SCCM include Ansible from Red Hat[32]. Both are leaders in the Forrester Wave and have a large market share[33]. Microsoft SCCM was deemed optimal over Ansible due to the availability of additional Microsoft solutions within System Center such as SCOM and SCSM.

SCOM on the other hand provides the CSIRT with the ability to monitor the health and performance of every service, operation, applications and devices in a constituency. The CSIRT will also attain the capability to perform recovery actions

[27] `https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-text-log?tabs=portal`, visited 13.05.2023

[28] See: `https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-iis-logs`, visited 13.05.2023

[29] See: `https://mortenknudsen.net/?p=1438`, visited 14.05.2023

[30] `https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center`, visited 16.05.2023

[31] `https://www.techtarget.com/searchwindowsserver/definition/Microsoft-System-Center-Configuration-Manager-2012`, visited 15.05.2023

[32] See: `https://www.ansible.com/`

[33] See: `https://www.ansible.com/blog/a-deeper-look-red-hat-named-a-leader-in-the-forrester-wave`, visited 14.05.2023

if an application or service malfunctions[34].

SCOM will support functions included in the Data Acquisition service under the Situational Awareness service area (see Appendix F). Alternatives to SCOM include Nagios XI, which provides several of the same functions. Both SCOM and SCCM offer seamless integration advantages due to their affiliation with Microsoft. However, it is important to note that Nagios offers a free version of Nagios XI, which stands in contrast to the comparatively high cost associated with SCOM.

Lastly, SCSM serves as a valuable tool for organisations seeking to adopt service management best practices. Central to accomplishing this is the utilisation of a CMDB (2.5.8). The CMDB houses essential information that holds significant value, enabling the CSIRT and its constituencies to keep track of configuration and ownership of sensors and devices. Although ServiceNow is a good alternative to System Center Service Manager (SCSM), the inclusion of SCSM within System Center justifies its utilisation alongside SCCM and SCOM.

5.4 Database Solution

As previously mentioned, Figure 5.1 demonstrates how the CSIRT will perform its data collection, and that the SIEM is dependent on vast amounts of data to perform its desired functions. This data requires a solution for storage, as well as a method for the SIEM to retrieve said data. With any SIEM, this data can either be stored through databases on-premises, in the cloud or both[35] . However, as previously explained, Microsoft Sentinel is a cloud native SIEM solution, and therefore also utilises a cloud environment for its storage purposes. These cloud environments are known as workspaces, and are currently only supported in public clouds[36].

Azure Log Analytics workspace is a part of Azure Monitor, which is Microsoft's solution for collecting, analysing, and responding to data collected from sensors in an environment[37]. The Log Analytics workspace is a required data storage solution for Sentinel to ingest data and perform its desired functions[38]. In reference to Figure 5.1, the appropriate database solution in the CSIRTs architecture is therefore Azure Log Analytics.

Several factors need to be considered when opting for a storage solution in a SIEM-based architecture. One of the most significant factors is the ability of the database solution to support a wide range of data types typically processed by a SIEM. Additionally, it is important to account for the speed of data transfer, as this can affect the ability of the SIEM to effectively identify and respond to potential

[34] See: `https://www.intelegain.com/what-is-microsoft-scom-and-sccm-and-how-do-they-differentiate/`, visited 14.05.2023

[35] See: `https://www.exabeam.com/explainers/siem/siem-architecture/`, visited 07.05.2023

[36] See: `https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/azure-monitor-workspace-overview`, visited 12.05.2023

[37] See: `https://learn.microsoft.com/en-us/azure/azure-monitor/overview`, visited 13.05.2023

[38] See: `https://learn.microsoft.com/en-us/azure/sentinel/prerequisites`, visited 12.05.2023

security incidents. Another crucial aspect is the capacity of the storage solution to handle large volumes of data over time, which can play a critical role in detecting and responding to persistent threats. Through the use of the Azure Monitor platform, and the Log Analytics workspace within, these mentioned factors can be met. A wide range of data types can be ingested from various types of sources, including Azure resources, on-premises resources, and other third-party sources. Furthermore, the use of agents and connectors allow for the collection and ingestion of data in near real-time. And as with other Azure resources, it provides scalable and flexible options in terms of data storage capacity[39].

5.5 Visualisation of Data Collection With the Proposed Components

Figure 5.6 demonstrates the data collection process of the CSIRT after the proposed components have been implemented. Relevant clients to Digdir's potential CSIRT have been added. "Altinn" is one of Digdir's common solutions and is an internet portal for digital dialogue between businesses, private individuals and public agencies[40]. "Brønnøysundregistrene" is a government body that provides order and overview of information on financial issues, ownership and liability in businesses[41]. "Skatteetaten" is the Norwegian tax administration. Finally, "ID-Porten" is another one of Digdir's common solutions, which offer Norwegian residents the same login functionality to services across the public sector[42]. All of these four organisations are overseen by Digdir, and could potentially become constituents to Digdir's CSIRT.

Recommended sensors have also been added, however, given that Figure 5.4 demonstrates the entire sensor architecture, only an overview is included in this figure. From the sensors, data is sent to the CSIRT. The greatest change from Figure 5.1 is the implementation of a cloud environment, which covers a substantial part of the components. In the cloud environment Microsoft Sentinel is added as the CSIRT's SIEM, with Microsoft 365 Defender as its XDR. Furthermore, Azure Monitor and Log Analytics is the database solution required of Sentinel, as previously explained. What is also important to note in this updated figure, is the relationship between Log Analytics, M365 Defender, and Sentinel. These three components work together in detecting and responding to potential security incidents. Finally, MISP is included as the CSIRT's Threat Intelligence Platform.

[39] See: https://learn.microsoft.com/en-us/azure/azure-monitor/data-platform, visited 13.05.2023

[40] See: https://www.altinn.no/om-altinn/hva-er-altinn/

[41] See: https://www.brreg.no/en/about-us-2/our-mission/

[42] See: https://samarbeid.digdir.no/id-porten/dette-er-id-porten/58

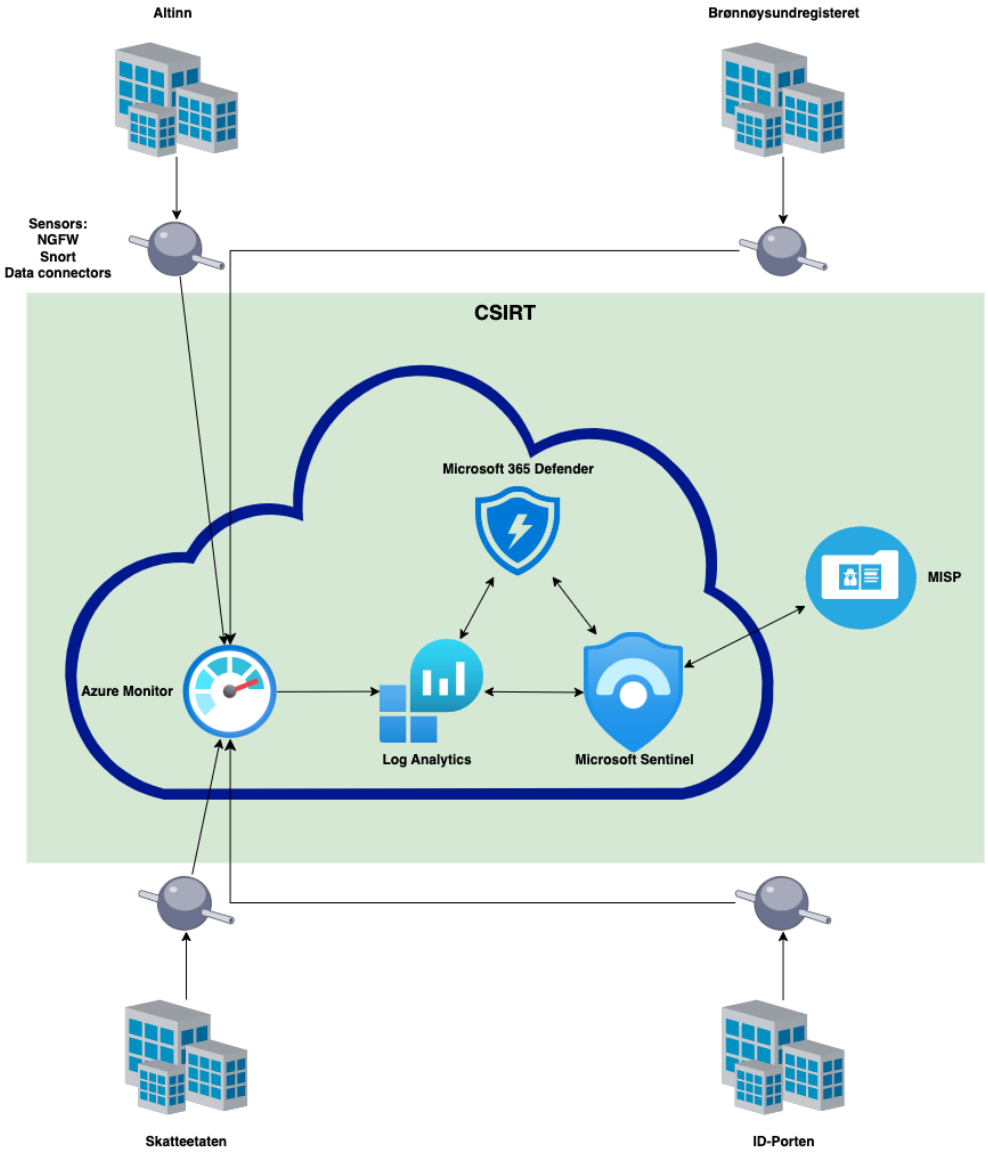


Figure 5.6: Proposed data collection architecture (created in diagrams.net)

5.6 Solutions for Incident and Vulnerability Analysis

The analysis of incidents and vulnerabilities is a crucial part of a CSIRT's operations. From this analysis, the CSIRT can acquire valuable insights into potential or realised vulnerabilities that may put a constituent at risk, and thereby assist in the mitigation and recovery from security incidents. This section will explore some of the components necessary to effectively perform this task, from analysing incidents that have taken place, to increasing knowledge and awareness around vulnerabilities that may compromise a constituent's systems.

5.6.1 Artefact and Forensic Evidence Analysis

As mentioned in Chapter 4, artefacts and forensic analysis is an important part of the Information Security Incident Management service area. The components presented in this section therefore support a variety of integral functions within the service area (see Appendix F).

Virtual Machines

Two specific virtualisation solutions were deemed optimal for the CSIRT's needs: the Sans Investigative Forensics Toolkit (SIFT) and FLARE VM.

SIFT Workstation is a VM distribution created by the SANS Institute for performing digital forensics[43]. SIFT provides a wide selection of freely available and open-source incident response and forensic tools, all in one solution[47]. These are most of the tools needed to conduct digital forensics, which makes it an advanced and convenient solution for the CSIRT. Some of the forensics tools included in the SIFT Workstation are[47]:

- **Plaso/log2timeline** – for timeline creations
- **Rekall/Volatility Framework** – for memory analysis
- **SleuthKit** – for analyzing disk images and extracting/recovering data
- **Various libraries** – for accessing different file formats
- **QEMU** – for emulating a system on a guest OS

The listed tools are just a small part of what SIFT has to offer, hundreds of additional tools for both incident response and digital forensics are included in the distribution. The comprehensiveness, functionality and practicality of the solution makes it an optimal component to implement in Digdir's CSIRT, in regard to artefact and digital forensic analysis.

Unlike SIFT, which is an Ubuntu based distribution, FLARE VM is Windows based. It is also freely available and open-source, with a collection of various tools required of a digital forensic team. FLARE VM was developed by a team at Mandiant and is designed to perform malware analysis, which is an integral process

[43]Note: SIFT is also available as a direct download for Ubuntu and Windows via Windows Subsystem for Linux. See: `https://www.sans.org/tools/sift-workstation/`

in artefact and digital forensic analysis. According to Mandiant, some of the tools provided with FLARE VM are[48]:

- **Debuggers** – for inspection of code on a lower lever
- **Disassemblers** – for translating code into assembler language
- **Decompilers** – for translating code to a higher, more human readable, level
- **Utilities for analysis** - for both static and dynamic analysis
- **Others**

FLARE VM was made to solve the problem of reverse engineering tool curation[44]. In cyber security, reverse engineering is a process which allows forensicators (and others) to study malware and dissect it, thereby gaining an understanding of the malicious software's functionalities. In this area, FLARE VM was deemed optimal for the CSIRT's solution for the same reasons as SIFT; it is an advanced and convenient all-in-one solution.

The justification for both SIFT and FLARE VM as components for the CSIRT's artefact and forensic operations, is due to the fact that they rely on different base OSs. According to a study conducted by AV-TEST, 83.45% of all malware in 2020 targeted the Windows OS[49]. Having a solution that can support the functionalities Linux brings, while at the same time being able to address Windows' susceptibility to attacks, was deemed the optimal solution.

Digital Forensics Artifacts Repository

After a security incident has occurred, remnants of the intruder attack may exist on the affected systems. These remnants are known as artefacts. According to FIRST, these artefacts can include executables, scripts, files, images, configuration files, tools, tool outputs, logs, etc.[2]. The Digital Forensics Artifacts Repository is a knowledge base of known digital artefacts that can be of use to the CSIRT in its forensic investigations. For instance, it can be utilised alongside other digital forensic tools like those collected from SIFT and FLARE VM, thereby enhancing the analysis and investigation process by leveraging the free, community-sourced, and machine-readable repository as an additional information source[50].

Hansken

Hansken is a digital forensic platform developed by the Netherlands Forensic Institute (NFI)[45]. In comparison to the Digital Forensics Artifacts Repository, Hansken is a more comprehensive and sophisticated forensic data solution. The core of the platform is a database that contains vast amounts of seized materials from criminal cases[51]. These seized materials are processed artefacts that have previously been used in cyber attacks. When investigating an incident, an analyst can send the affected artefact(s) as forensic copies to the platform for processing. The

[44] See: `https://github.com/mandiant/flare-vm#readme`, visited 15.05.2023

[45] See: `https://www.forensicinstitute.nl/products-and-services/forensic-products/hansken`, visited 14.05.2023

process extracts data and metadata as traces and stores it in a centralised database[52]. Once a trace has been created, the analyst can apply filters and initiate special queries to gather relevant data related to the incident to aid in forensic investigation. Kripos, the Norwegian National Criminal Investigation Service, is currently one of multiple law enforcement agencies that are international partners of Hansken[46]. This indicates the tool is proven and tested, as well as facilitating cooperation between Digdir's CSIRT and Norwegian law enforcement.

5.6.2 Vulnerability Analysis

Vulnerability analysis constitutes a significant aspect within the Vulnerability Management service area of the FIRST framework. The essential components and processes involved in proficient vulnerability analysis thus support a considerable part of its functions (see Appendix F). Vulnerability analysis naturally encompasses various additional operations, including the discovery and subsequent response to the vulnerabilities. Consequently, tools pertinent to these operations are equally applicable to the process of vulnerability analysis.

Vulnerability Assessment Solutions

For Digdir's CSIRT to provide accurate, comprehensive and timely vulnerability management, solutions are needed to enhance the discovery of potential vulnerabilities. A vulnerability assessment solution is a tool that when implemented, can identify, categorise and manage vulnerabilities. According to Gartner, two of the leading providers for such a solution are: InsightVM and Nessus[47].

InsightVM is a vulnerability assessment tool developed by Rapid7, which has been recognised by both Gartner and Forrester as a quality choice in terms of vulnerability management[48]. It incorporates several features for assessing, monitoring and remediating vulnerabilities, and with its REST API it can easily be integrated into the CSIRT's environment[49].

Nessus, developed by Tenable, is Rapid7's main competitor in vulnerability assessment solutions. Like InsightVM, it is also widely recognised as a quality solution. Nessus' platform contains a variety of features that can assist the CSIRT in its vulnerability management. Furthermore, Nessus can seamlessly integrate with Microsoft services. Notably, it can be integrated with the proposed SIEM solution, Microsoft Sentinel, which combines the insight of Nessus with Sentinel's SIEM functionalities[50]. A solution in addition to InsightVM or Nessus could be Microsoft

[46] See: https://www.hansken.nl/hansken-community/partners

[47] See: https://www.gartner.com/reviews/market/vulnerability-assessment

[48] https://www.rapid7.com/about/press-releases/rapid7-named-a-leader-in-vulnerability-risk-management-report and https://www.gartner.com/reviews/market/vulnerability-assessment

[49] See: https://www.rapid7.com/products/insightvm/features/, visited 15.05.2023

[50] https://www.tenable.com/partners/technology, visited 15.05.2023

Defender Vulnerability Management. Opting for Microsoft as a vulnerability assessment tool would be a logical solution given the proposed CSIRT architecture demonstrated in Figure 5.6, considering the abundance of other Microsoft components. However, Microsoft's solution is not yet commercially available[51]. Opting for either InsightVM or Nessus is therefore deemed a sensible solution for Digdir's CSIRT.

Common Vulnerabilities and Exposures Database

Common Vulnerabilities and Exposures (CVE) is a catalogue of publicly known information security vulnerabilities. CVE's operation is to identify, define, and catalogue these vulnerabilities[52]. The information derived from CVE can be applied by Digdir's CSIRT in two primary manners. One approach is by keeping up to date on the CVE database to increase awareness on confirmed vulnerabilities that may affect its constituents. Another approach involves integrating CVE's data into other components to automate vulnerability management or leveraging external systems that utilise the CVE database for the same purpose. The following two systems are examples of systems that make use of CVE for their purposes. These should be implemented by the CSIRT in addition to CVE, to ensure effective vulnerability management.

Exploit Prediction Scoring System

The Exploit Prediction Scoring System (EPSS) is a method for measuring exploitability, i.e., the likelihood that any software vulnerability, anywhere, will be exploited. EPSS is a data-driven system that ingests data from CVE, and then uses this threat information, as well as real-world exploit data, and applies it to its scoring system[53].

The CSIRT should utilise EPSS as a prioritisation tool in its vulnerability analysis operations. The EPSS provides a score from 0 to 1, where a higher number indicates an increased probability of exploitation. The data EPSS produces, as well as the score, provides the CSIRT with valuable insight, which can be applied to its own environment to determine the likelihood of potential vulnerabilities getting exploited at its constituencies.

National Vulnerability Database

The National Vulnerability Database (NVD) and EPSS share similarities in various ways. NVD is also a system that provides data relevant to vulnerability management based on CVE analysis[54]. As with EPSS, this data is valuable information

[51] `https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide`, visited 13.05.2023

[52] See: `https://www.cve.org/About/Overview`

[53] See: `https://www.first.org/epss/`, visited 14.05.2023

[54] See: `https://nvd.nist.gov/general`

to the CSIRT, and can also be applied to its vulnerability management services. By using NVD's API, data can be retrieved and used in context with the CSIRT's vulnerability environment.

5.7 Communication

As mentioned in Section 2.5.7, communication plays a critical role in the CSIRT's ability to relay their information out to constituents or other parties. This naturally translates to several of the different service areas and services of the FIRST framework, most notably in Situational Awareness. However, communication also plays a substantial part in Information Security Incident Management and Vulnerability Management (see Appendix F).

5.7.1 Visualisation of Communication Between the CSIRT and Constituents

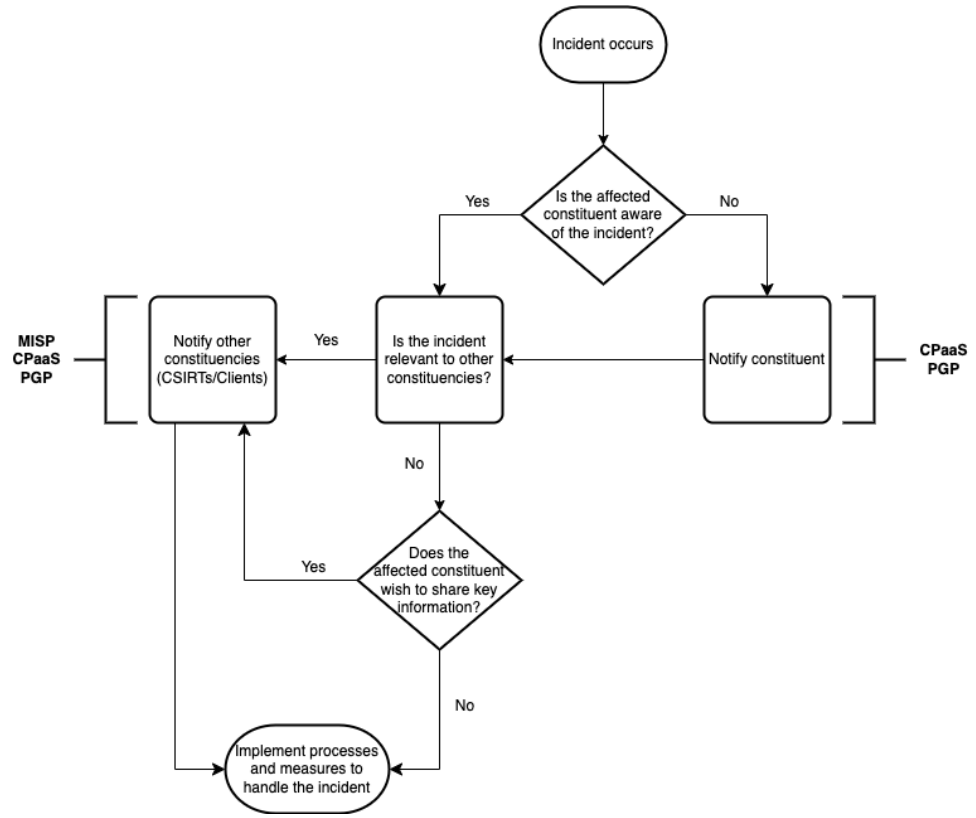


Figure 5.7: Case of communication following an incident (created in diagrams.net)

Figure 5.7 is an example on how the CSIRT might conduct its communications with constituents if an incident occurs. An incident can be discovered by the

CSIRT, in which case they need to notify the affected constituent, or the CSIRT can be contacted by the constituent seeking assistance and guidance regarding a potential security incident. Communication with a constituent can be done through a Communication Platform as a Service (CPaaS, 2.5.7) or PGP encrypted messages, both of which are integral components in the proposed CSIRT environment regarding communication.

It is important to note that when a security incident occurs, it is the affected constituent that fully owns the incident (Appendix E). This essentially means that it is up to the affected constituent whether they wish to share any information about the incident or not. Sharing key information on a security incident can be valuable information to other CSIRTs and organisations in the same sector as the affected constituent. Although it is not recommended, a constituent may wish to withhold this information in order to protect its own reputation. Should the constituent wish to share information, the CSIRT could also make use of CPaaS or PGP to communicate this to other clients, as well as the use of MISP to other CSIRTs.

5.7.2 Cisco Webex (CPaaS)

Cisco Webex is a cloud-based communication platform that delivers all the necessary features of a communication service. The product facilitates common capabilities such as text chat, voice and video calls, and file and screen sharing[53]. While this is what to be expected from a CPaaS, Cisco Webex also allows the use of advanced messaging. Based on Gartner's Market Guide for Communications Platform as a Service, this includes the use of RCS (Rich Communication Service), verified SMS, email and social media messaging[18]. Webex also offers a great range of integration with other solutions such as Google, Microsoft, and Slack. This set the foundation for their omnichannel solution, which allows the CSIRT to seamlessly collaborate with colleagues, constituents, and third-party entities regardless of the platform they are using.

Another important factor to keep in mind when selecting the communication platform is security. With the growing number of organisations communicating online and remotely, security has become a top priority. Webex offers a great deal of security by using E2EE (End-To-End Encryption) on all communications related to the portal, this includes text, voice, video, and data. Based on a report from the NSA (National Security Agency) they are one of the few vendors that offer E2EE in all these areas as well as being certified by FedRAMP[54]. FedRAMP being a US standardisation program for secure cloud services[55]. While this is mainly related to the US, they are also compliant with other industry regulations, such as GDPR and a number of ISO/IEC security certifications[56].

[55] Federal Risk and Authorization Management Program. See: `https://www.fedramp.gov/`

[56] See: `https://www.webex.com/security.html`, visited 13.05.2023

5.7.3 Best Practical Request Tracker for Incident Response

The Best Practical Request Tracker for Incident Response (RTIR) is a supporting communication tool developed in collaboration with the UK-based Janet CSIRT[57]. Its is an open-source ticketing tool used to initiate and track incident handling both from the CSIRT and its constituents. The component is based on the original RT (Request Tracker) platform and utilizes the REST API to allow integration with existing solutions, such as Microsoft Sentinel[58]. The main purpose of the tool is to increase the effectiveness of incident tracking and have a clear view of the workflow.

5.7.4 Pretty Good Privacy

When a constituent needs to contact the CSIRT and the message contains confidential information, such as incident reports or personal information, it is recommended to use PGP encryption. PGP is a security program for encryption and decryption of messages through digital signatures and file encryption[59]. It is most commonly used in connection with email communication and uses a combination of symmetric and public-key encryption. Both users on either end of the communication are assigned randomly generated public and private keys. Which are then used to authenticate the intended recipient. Only the intended recipient will have the specific private key needed to decrypt the message[60].

The use of PGP encryption is a common practice in CSIRTs. Both FIRST and NCSC make use of PGP for cryptographic communication with their constituencies[61]. It is also recommended that Digdir does so, to ensure the privacy and confidentiality of the CSIRT, as well as its constituents. In doing so, Digdir's CSIRT would have to make their public key public and educate their constituencies on how to make use of PGP. A program that can be used for this matter is GnuPG, which is an open-source software that implements PGP through the OpenPGP standard[62]. OpenPGP is a standard set by the Internet Engineering Task Force (IETF) in RFC 4880, allowing for the use of PGP while eliminating the need to license it, as PGP is a patented product[55].

5.7.5 Traffic Light Protocol

Another good practice when exchanging sensitive information, or any information, is to use the Traffic Light Protocol (TLP) system. TLP is a system which classifies sensitive information to facilitate greater sharing of information, even

[57] `https://beta.jisc.ac.uk/csirt`, visited 16.05.2023

[58] `https://bestpractical.com/request-tracker`, visited 16.05.2023

[59] See: `https://www.fortinet.com/resources/cyberglossary/pgp-encryption`, visited 10.05.2023

[60] See: `https://www.upguard.com/blog/what-is-pgp-encryption`, visited 10.05.2023

[61] See: `https://www.first.org/pgp/`. and `https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/kontakt-ncsc/`

[62] `https://gnupg.org/`

information that might be regarded as sensitive[56]. Information is divided into four labels, based on the sensitivity of the information being shared: Red, Amber, Green and Clear. Table 5.1 provides a detailed explanation of each TLP colour[57]:

Table 5.1: The meaning behind and usage of the TLP colours

Colour	TLP: RED	TLP: AMBER	TLP: GREEN	TLP: CLEAR
Meaning	Not for disclosure	Limited disclosure	Community-limited disclosure	Unlimited disclosure
When to use	When the disclosure of information poses substantial risks to the privacy, reputation, or operations of the organisations involved	Only within the organisation and its client on a need-to-know basis	When information is needed to increase awareness within a wider community. Not via publicly accessible channels.	When information has minimal to no foreseeable risk of misuse. In accordance with relevant rules and procedures, this information can be shared with the public.

Similar to PGP, TLP is also a common practice regarding information sharing in a CSIRT. All communication, vertical and lateral, as shown in Figure 2.1, should be marked with a TLP colour relevant to the information being shared. Constituents of the CSIRT need to be educated and made aware of the meaning and purpose behind these colours, to ensure the confidentiality and security of all parties involved. A common practice within NCSC is to regard all information being shared in and with NCSC as TLP:AMBER, unless otherwise specified[63]. It is recommended that also Digdir incorporate the TLP system in its operations. As mentioned, TLP will maintain confidentiality between the CSIRT and its constituents. Furthermore, to prevent information leaks on threat intelligence, TLP can also be integrated with MISP, facilitating greater lateral information sharing between CSIRTs[58].

[63] See: `https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/kontakt-ncsc/retningslinjer-for-deling-av-informasjon/`, visited 10.05.2023

5.8 Solutions for Training, Education and Awareness Building

A key component of establishing a competent and resilient CSIRT lies in providing adequate training and education, as well as processes for building awareness for both its employees and its constituents. The components required for these operations play a pivotal role in supporting the functions of the Situational Awareness and Knowledge Transfer service areas (see Appendix F). This section will delve into these components in greater detail, showcasing their significant contribution to the CSIRT.

5.8.1 KnowBe4

KnowBe4 is a security knowledge mapping and education tool that can assist the CSIRT in accomplishing multiple functions in the Knowledge Transfer service area (see Appendix F). The tool was recognised as a leader in Security Awareness and Training Solutions by Forrester in 2022[64]. Alternative tools to KnowBe4 are Microsoft Forms, Articulate 360, and Sophos[65]. However, many of these solutions are not as widely adopted, given that they lack some of the core features and ease of integration one gets with KnowBe4.

Services in the FIRST framework such as Awareness Building, Exercise, and Training and Education, suggest that a CSIRT require methods for identifying knowledge gaps in its constituencies. KnowBe4 is a valuable solution to fulfil this requirement. To facilitate identification of knowledge gaps, Knowbe4 uses Security Awareness Proficiency Assessments (SAPA) and Security Culture Surveys (SCS). SAPA is a way to assess in what grade employees are susceptible to cyber attacks by testing their knowledge in areas such as[59]:

- Email Security
- Incident Reporting
- Internet Use
- Mobile Devices
- Passwords and Authentication
- Security Awareness
- Social Media Use

SCS's focus is on the security culture among employees and includes topics such as attitude, behaviour and communication. Data gathered from SAPA and SCS need to be present in a comprehensible manner through visualisation, which KnowBe4 provides[59].

After information has been gathered about knowledge gaps, the CSIRT can begin creating and distributing training material and exercises to either entire

[64] See: `https://www.knowbe4.com/forrester-wave-security-awareness-training`, visited 13.05.2023

[65] See: `https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/knowbe4/alternatives`, visited 13.05.2023

constituencies or specific employees. KnowBe4 already has existing libraries of content the CSIRT can use as educational material and is presented through a browser-based platform, rendering it readily accessible[60]. The educational material can be presented to the constituencies in multiple ways including interactive modules, videos, games, posters and newsletters[66]. Having access to libraries can lessen the workload on the CSIRT's employees when training constituencies about overall security knowledge, which might improve staff retention.

Using existing libraries pre-developed with training material is limiting. This is du to the fact that some security knowledge is too specific and the CSIRT will therefore need functionalities to create custom material. To facilitate this KnowBe4 provides SCORM-compliant LMS functionality[60]. SCORM stands for Sharable Content Object Reference Model and is a standard for E-learning products. Learning Management Systems or LMS are platforms where SCORM content can be viewed and managed[67]. This provides the CSIRT with the option to export material to other LMSs making it easier to change platform in the future and facilitates the storing of training material on different platforms.

Providing the constituencies with security awareness information is insufficient to drastically improve security knowledge. The CSIRT's goal should be to make the constituencies gain experience on cyber security and threats. Experience is knowledge acquired within a time period of practical experiences, which comes with time, exposure, and practice. KnowBe4 facilitates exposure and practice as it provides several exercises that can be forwarded to employees on a regular basis, providing the CSIRT and constituencies with training material that fulfil integral functions of the FIRST framework.

5.8.2 CSIRT Employee Development

Employee development is crucial for the CSIRT as it necessitates the continual enhancement and maintenance of the knowledge of its personnel, in addition to fostering networking opportunities both within and outside the organisation. By investing in employee development, the CSIRT ensures that its team members stay abreast of the latest industry trends, emerging threats, and advanced incident response techniques. This ongoing learning and skill-building process enable CSIRT personnel to adapt swiftly to evolving cyber threats and effectively respond to incidents with precision and expertise, as a result operating in accordance of the functions under the Knowledge Transfer service area of the FIRST framework (see Appendix F).

Section 2.7 on human aspects mention the usage of both internal and external development methods. Mentoring tools such as MentorCloud and practices such as job shadowing can help facilitate internal development. MentorCloud

[66] See: `https://www.knowbe4.com/en/products/enterprise-security-awareness-training/`, visited 14.05.2023

[67] See: `https://scorm.com/scorm-explained/one-minute-scorm-overview/`, visited 15.05.2023

is an automated tool that seamlessly matches mentors with mentees, providing them with subject-specific guidance, goal-oriented support, and valuable feedback throughout their mentorship program[68]. Job shadowing is the practice of observing another employee performing their roles and is usually used to onboard new employees, allowing them to gain firsthand insights into job responsibilities, organisational processes, and the overall work environment, thereby accelerating their learning curve and fostering a smoother transition into their new roles[69].

External development can be facilitated by using certification programs and attending conferences on subjects relevant to cyber security. Certifications that are relevant to incident response specialists include:

- CERT-Certified Computer Security Incident Handler (CERT-CSIH)
- Certified Information Systems Security Professional (CISSP)
- Certified Reverse Engineering Analyst (CREA)
- Cisco Certified Network Associate (CCNA)
- GIAC Certified Forensic Examiner (GCFE)

By obtaining these certifications and attending relevant conferences, incident response specialists gain specialised knowledge, industry recognition, and a competitive edge, empowering them to effectively tackle incidents and contribute to maintaining robust cyber security postures within the CSIRT. In addition to these certifications, NSM also provides courses that could be highly relevant in increasing the knowledge of the CSIRT's employees, as well as material that could be recommended to its constituents[70]. Internal and external development tools support key functions under Traning and Education in Knowledge Transfer (see Appendix F).

[68] See: https://www.mentorcloud.com/mentor-platform

[69] See: https://www.gartner.com/en/human-resources/glossary/job-shadowing

[70] See: https://nsm.muniolms.com/no/shop/nsm

Chapter 6

Discussion

In this chapter the researchers discuss several aspects related to the thesis, including some of the choices made throughout the research process, limitations encountered, and reflections on the FIRST framework.

6.1 Choice of Components

The selection of appropriate components to establish a CSIRT environment is a challenging endeavour, primarily due to the abundance of options available in the market, each promising to offer the best solution in their area of expertise. Furthermore, factors such as functionality, compatibility with other components, ease of use, and scalability, in ensuring that a solution was suitable to Digdir's needs, contributed to making this process challenging. Thus, the price of the components were not a factor in the selection proccess. As a result, the cost-effectiveness of a component did not affect its likelihood of being proposed to Digdir, even if it happened to be the most expensive option available. As the task was a literature study, the researchers were limited to their own information gathering abilities when determining the optimal components. This meant that it was imperative to have good sources to rely on when making decisions.

Considering Digdir's unique requirements was something to keep in mind when selecting components. There are several factors to consider that can drastically affect an overall solution. The optimal way would be to do a thorough analysis of the organisation's existing systems and infrastructure. This would be of great help in finding compatibility and integration solutions. Although a detailed overview of the existing systems was not provided, it was mentioned that certain solutions, such as Azure, was in use. This played a significant factor in the selection process in choosing components that could integrate with the solution. The proposed solution of a Microsoft SIEM and XDR was therefore a natural choice. While other solutions such as Splunk Enterprise Security, IBM QRadar, CrowdStrike Falcon Insider and Palo Alto Cortex had similar capabilities (see Appendix F), the Microsoft solution provided a more seamless integration. However, there is still

the potential of licensing complexities and function overlaps. The licensing for Microsoft product can be intricate and is something that Digdir must keep in mind if opting for this solution. To remedy this, they may need to consult with licensing experts in order to get the desired functionality and capabilities. This is also apparent considering function overlaps. The proposed solution has sought to minimise function overlap between the SIEM and XDR, however, some level of overlap may still exist. The function overlaps may not cause any problem to the functionality, but rather add redundancy, which may be unwanted as it uses unnecessary resources. In order to locate overlaps, the optimal way would be to test the solution and analyse how every component interacts with each other.

6.2 Use of Sources

The strength of a literature study relies on its sources. It was therefore crucial that this study was supported by credible sources. The sources used in this study ranged from vendor-provided information, third party reviews, and mentions in relevant academic literature. The use of vendor-provided sources proved useful in finding and understanding the technical capabilities of a product. Vendors often provided documentation on specific requirements and functionalities that proved useful when comparing solutions. It is however important to acknowledge that these documents may exhibit a bias towards their respective products, particularly evident in the overstatement of their capabilities. Consequently, a critical examination of alternative sources was imperative to substantiate our recommendations.

By utilising sources such as Gartner and Forrester, the study had a more impartial evaluation of the components. As these reports are updated regularly and utilise a comprehensive evaluation methodology, they were deemed as trustworthy sources. It proved especially useful in decision making. If two components were regarded as viable options, an external source could determine the outcome. Importantly, it should be noted that third party sources can have a lack in scope regarding all aspects of the task. While Gartner Magic Quadrants, Gartner Market Guides, and Forrester Waves were good additions in evaluating some components, The reports could be seen more as a general overview as they often relied on the same publicly available information, and consequently lacked depth. This is to some extent negated by incorporating reviews from active users of the product to provide better insights. These sources may also have limitations, such as not encompassing all potential vendors offering the given solutions. The extensive number of vendors in the market makes it infeasible to include every one of them. While these sources strive to maintain impartiality, they can still be influenced by vendor relationships and prevailing market trends. To address this, the overall evaluation incorporated information from supplementary sources to ensure a comprehensive and unbiased assessment.

6.3 Limitations

Reputable, reliable and credible sources were even more important given the limitations of the study. The researchers were not able to test any of the components mentioned on their own, which resulted in a substantial reliance on publicly available information, reputable sources and product reviews. With a limited time to conduct research, it was crucial to maximise the utilisation of trustworthy sources to compensate for the inability to perform direct testing. By doing so, the researchers ensured the integrity and accuracy of the gathered information, despite the limitations imposed by lack of testing and time constraints.

Testing the solution in practice would have given a more reliable analysis of how every component worked in correlation to each other. This could provide valuable information on potential challenges with the solution and unforeseen issues. The data gathered from such testing would allow for a more objective evaluation of the functionality and performance of the components. However, performing such tests requires significant resources, which exceeded the scope of the assigned task.

6.4 Implementation of Framework

6.4.1 FIRST CSIRT Services Framework

The FIRST framework offers an extensive range of capabilities, making it a comprehensive framework that effectively addresses the requirements of a CSIRT. The framework was used as a structured approach to identify and evaluate components required for the task. Employing this framework ensured that all components served a purpose and played a functional role. The task giver wanted a complete set of tools to establish a CSIRT for Digdir, thus emphasising the importance of identifying components that cater to each service and function outlined in the framework.

It is however interesting to note that not all services in the framework are necessary to perform the duties of a CSIRT. The FIRST framework addresses that no CSIRT is expected to provide every service described to its constituents[2]. There is still a set of services that a CSIRT should provide. ENISA defines incident and artefact analysis, incident and vulnerability coordination, and awareness building as typical services a CSIRT should have at a minimum[3]. This prioritisation of services, might create the impression that service areas such as situational awareness and information security event management are less crucial for a CSIRT. While this could be accurate in most situations, it can be due to the assumption that organisations seeking to establish a CSIRT may already have existing solutions that cover these specific service areas. In such instances, the CSIRT would simply need to adopt or rely on the utilisation of these pre-existing solutions.

This was not a factor regarding the task given by Digdir, as they wanted a proposed solution for a complete CSIRT environment. The proposed solution is

a comprehensive one, however, that does not mean all services need to be implemented at the same time to function. Based on the FIRST framework, Digdir could prioritise which service they deemed most important and issue an incremental service implementation. A proposed prioritisation could be the minimal services according to ENISA, together with a data collection and communication solution. An incremental implementation would work for most of the components, as they generally do not have any significant dependencies on other components.

6.4.2 FIRST CSIRT Roles and Competencies

In Appendix F, each function of the framework is assigned with a specific role. These roles are directly derived from the FIRST CSIRT Roles and Competencies Framework[26]. Given that the report already built upon the FIRST CSIRT Services Framework, it was a logical choice to use FIRST once more for this purpose. This was important as some of the functions did not have a clear tool or component that would fulfil its purpose. The use of the additional framework ensured that the proposed solution had better coverage and eliminated uncertainties from undefined functions. Within our solution, we identified a total of 17 functions classified as employee functions. Alternatively, these roles could be referred to as expert functions, given their reliance on the expertise and knowledge of the assigned role. The roles overlap in the different service areas much like the technical components. The overlapping showcases how collaboration and information sharing is crucial to the effectiveness of a CSIRT. It highlights that successful incident response is not solely dependent on the efforts of individual team members, but rather on their ability to collaborate and work together across diverse areas of expertise.

An important note is that one role does not specify a single employee of the CSIRT. While the roles in the framework encompass expertise and responsibilities needed to fulfil specific functions, multiple individuals may contribute to one role. This can be the case for roles such as the incident analyst, where multiple employees may contribute as a smaller team working together. However, this is all dependent on the workload and responsibilities of the CSIRT. Since Digdir has multiple constituencies that provide critical national functions, they may need to have multiple smaller teams working within the same roles to ensure efficient support. Alternatively, an individual can also assume multiple roles in the CSIRT.

6.5 Reflection on the Collaborative Approach

The group collaboration has been highly effective, with most of the tasks completed through close proximity, either in-person on campus or utilising online tools. This made it easy to follow what each team member's activity was, and eliminated the need for a project management tool. The project plan in Appendix B states that we would use Scrum to divide the task into smaller sprints. This has

worked well and has made it easier for the group to move on to new research areas and effectively allocate time.

Despite the use of Scrum in an effort to distribute the workload over time, we found ourselves not always completing the sprints in the allocated time, and working more intensively as the deadline approached. This is evident in our timesheet (see Appendix J), which reflects extended periods of work on certain days to meet our objectives. For instance, the initial research sprint required significantly more effort than originally anticipated, leading to a delay of approximately 2-3 weeks in the project's timeline during its early stages. Consequently, this created a heavier workload towards the project's conclusion, which is an important lesson for the group to consider in future endeavors.

To ensure the report's quality, each group member has taken a critical approach to their own writing as well as that of their fellow group members. This has meant that the team learned a lot from one another as we have gone through the documentation process.

6.6 Learning Outcome

During the process of creating this report the group learned a lot about teamwork, writing and the use of sources in a literature study.

The project has been educating, in regard to the importance of prioritisation and recognising the constraints of time. In the initial weeks of the research phase, the objective was to delve extensively into numerous tools across various technological areas. This became evident as an unattainable objective, as understanding the intricate concepts of technologies such as SIEM, XDR, and IDS proved to be overwhelming. The mere act of delving into one of these technologies only seemed to deepen our confusion instead of providing clarity. Because of the time limitations the goal had to be limited.

The importance of communication and cooperation also became apparent as members of the group acquired knowledge on different technologies and solutions. The close proximity among group members made it easy to exchange knowledge and enabled us to seek clarification on concepts that other members had already gained an understanding of.

Finally, gaining insights into the effective utilisation of sources to back up the information presented in the report proved to be a valuable learning experience. Overleaf has proven to be an invaluable tool for facilitating the management and presentation of sources in a clear and comprehensible manner and using Overleaf has been a worthwhile endeavour, despite the initial time investment required.

Chapter 7

Conclusion

This chapter represents the concluding section of the report, wherein the researchers exlpore the potential for future advancements within the research area. Additionally, it encompasses the concluding remarks that encapsulate the overall findings and implications of the study.

7.1 Further Work

There is considerable potential to enhance the relevance of this report for organisations and Digdir through further work and refinement.

The next logical progression entails the practical experimentation of all identified tools to assess their functionality in real-world scenarios. Since the solution presented in this report remains predominantly theoretical, it is likely to unveil challenges in integrating and synchronising of various tools, despite the supplier's claimed compatibility. Additionally, it is essential to conduct comprehensive testing to verify whether the recommended tools genuinely deliver the functionalities advertised or if they have been exaggerated.

Another aspect of the report could have included an exploration of emerging technologies, such as Web3 and Cybersecurity mesh architecture (CSMA), as well as the growing trend of remote workers. These technologies are highlighted in Gartner's Hype Cycle and possess significant implications for organisational security both presently and in the foreseeable future[1]. Identifying their potential impact and investigating their implications would be a valuable focus for future research endeavours in this domain.

Additionally, one could conduct the study utilising a different framework, and subsequently compare the proposed solutions. This could be impactful, as the new edition of ISO/IEC 27035 was released early this year. Having multiple studies would provide further insight into the problem area, where one could evaluate

[1] See: `https://www.gartner.com/en/articles/what-s-new-in-the-2022-gartner-hype-cycle-for-emerging-technologies`., visited 18.05.2023

the capabilities of the respective frameworks to determine the optimal solution.

7.2 Closing Remarks

The aim of this study was to identify necessary components for establishing a well-functioning CSIRT service for Digdir. One of the criteria was to use a known framework so it could be easily applicable for Digdir. To achieve this, a literature study was conducted based on the FIRST CSIRT Services Framework. The framework served as a guide for selecting components aligned with each function. The validity of the sources was assessed using the CRAAP test to ensure validity.

Given the wide range of tools available, a comprehensive evaluation was carried out to identify the components best suited for the task. These components underwent assessments based on functionality and compatibility. The components found, support all of the functions in the FIRST CSIRT framework by including: data collection and management tools, incident and vulnerability analysis tools, as well as the means to coordinate and improve the efforts. It is important to acknowledge the limitations of the study, as it relied solely on publicly available information. Therefore, the evaluation had to be cross-examined with external sources to provide an impartial and comprehensive perspective.

The findings in the study presents a proposed architecture and implementation of the identified components. By implementing these components within the recommended architecture, Digdir can establish a CSIRT service based on the functions of the FIRST framework. As the study is purely theoretical, it was not in its scope to test the recommended solution in a real-word scenario. It would therefore be beneficial to conduct practical testing of the components further to confirm their effectiveness and compatibility.

Overall, this study contributes to the establishment of a CSIRT service for Digdir by providing a framework and implementation based on the FIRST CSIRT Services Framework. Through this approach, Digdir can enhance its incident handling capabilities and better safeguard its digital assets.

Bibliography

[1] The Royal Ministry of Local Government and Regional Development, *Tildelingsbrev 2023 – Digitaliseringsdirektoratet*, 2023. [Online]. Available: https://www.regjeringen.no/contentassets/7f9b178a808649dfad4bc4ae2401ae07/2023_tildelingsbrev-2023-digdir.pdf, Last accessed: 21.02.2023.

[2] FIRST.org, Inc., *Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0*, 2019. [Online]. Available: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf, Last accessed: 10.05.2023.

[3] E. Taurins, 'How to set up CSIRT and SOC,' European Union Agency for Cybersecurity (ENISA), 2020. [Online]. Available: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc, Last accessed: 15.03.2023.

[4] Nasjonal Sikkerhetsmyndighet, 'Rammeverk for håndtering av IKT-sikkerhetshendelser,' 2017. [Online]. Available: https://nsm.no/getfile.php/133853-1593022504/NSM/Filer/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf, Last accessed: 06.03.2023.

[5] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle and M. Zajicek, 'Handbook for Computer Security Incident Response Teams (CSIRTs),' Carnegie Mellon University, Software Engineering Institute, Tech. Rep., 2003. [Online]. Available: https://resources.sei.cmu.edu/asset_files/handbook/2003_002_001_14102.pdf, Last accessed: 10.02.2023.

[6] Cynet, *What is a Computer Security Incident Response Team (CSIRT)?* [Online]. Available: https://www.cynet.com/incident-response/what-is-a-computer-security-incident-response-team-csirt/, Last accessed: 27.02.2023.

[7] Imperva, *Advanced persistent threat (apt)*. [Online]. Available: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/, Last accessed: 04.04.2023.

[8] Cynet, *Advanced persistent threat (apt) attacks*. [Online]. Available: https://www.cynet.com/advanced-persistent-threat-apt-attacks/, Last accessed: 22.04.2023.

[9] CrowdStrike, *CROWDSTRIKE 2023 GLOBAL THREAT REPORT: EXECUTIVE SUMMARY*, 2023. [Online]. Available: https://www.crowdstrike.com/wp-content/uploads/2023/02/2023-Global-Threat-Report-Executive-Summary.pdf, Last accessed: 15.04.2023.

[10] Airbus, *Apt kill chain: Part 4 - initial compromise*. [Online]. Available: https://www.cyber.airbus.com/apt-kill-chain-part-4-initial-compromise/, Last accessed: 27.02.2023.

[11] Microsoft, *What is SIEM?* [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem, Last accessed: 15.04.2023.

[12] Exabeam, *A siem security primer: Evolution and next-gen capabilities*. [Online]. Available: https://www.exabeam.com/explainers/siem/a-siem-security-primer/, Last accessed: 15.04.2023.

[13] M. Stone, *XDR vs SIEM: A Technical Comparison*, 2022. [Online]. Available: https://panther.com/cyber-explained/xdr-vs-siem-a-technical-comparison/, Last accessed: 12.03.2023.

[14] Anomali, *What is a threat intelligence platform (tip)?* [Online]. Available: https://www.anomali.com/resources/what-is-a-tip, Last accessed: 24.04.2023.

[15] M. Rosner, *Vulnerability Management vs. Vulnerability Assessment*, 2023. [Online]. Available: https://www.rapid7.com/blog/post/2023/03/07/vulnerability-management-vs-vulnerability-assessment/, Last accessed: 04.05.2023.

[16] C. Constantine, *What to log in a SIEM: SIEM and security logging best practices explained*, 2020. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/what-kind-of-logs-for-effective-siem-implementation, Last accessed: 22.04.2023.

[17] A. Saravanan, *Log collection 101: Covering the basics*, 2022. [Online]. Available: https://www.manageengine.com/log-management/cyber-security/log-collection-101.html, Last accessed: 02.04.2023.

[18] L. Unden-Farboud, B. Doherty, D. O'Connell and A. Patankar, *Market Guide for Communications Platform as a Service*, 2022. [Online]. Available: https://www.gartner.com/document/4018801?ref=solrAll&refval=362161121, Last accessed: 19.04.2023.

[19] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington and C. Thomas, *MITRE ATT&CK: Design and Philosophy*, 2020. [Online]. Available: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy, Last accessed: 29.04.2023.

[20] Microsoft, *Understand security coverage by the MITRE ATT&CK® framework*, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage, Last accessed: 10.05.2023.

[21] A. Dufkova, D. Stikvoort, K. P. Kossakowski, M. Maj, V. Benetis and K. Gapinski, *ENISA CSIRT MATURITY FRAMEWORK UPDATE*, 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework, Last accessed: 15.04.2023.

[22] H. Duijnhoven, T. van Schie and D. Stikvoort, *Global CSIRT Maturity Framework: Stimulating the development and maturity enhancement of national CSIRTs*. [Online]. Available: https://cybilportal.org/wp-content/uploads/2020/02/Global-CSIRT-Maturity-Framework_v2_april-2021.pdf, Last accessed: 20.04.2023.

[23] D. Stikvoort, *SIM3 : Security Incident Management Maturity Model*, 2019. [Online]. Available: https://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf, Last accessed: 15.04.2023.

[24] C. Nobles, 'Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem,' *HOLISTICA – Journal of Business and Public Administration*, 2022. [Online]. Available: https://sciendo.com/article/10.2478/hjbpa-2022-0003, Last accessed: 16.04.2023.

[25] 'WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT?' Carnegie Mellon University, Software Engineering Institute, Tech. Rep., 2017. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485684.pdf, Last accessed: 20.04.2023.

[26] FIRST.org, Inc., *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies Version 0.9.0*, 2022. [Online]. Available: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf, Last accessed: 16.05.2023.

[27] National Institute of Standards and Technology, 'Workforce Framework for Cybersecurity (NICE Framework),' U.S. Department of Commerce, Tech. Rep. NIST Special Publication 800-181 Revision 1, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf, last accessed: 02.05.2023.

[28] R. V. der Kleij, G. Kleinhuis and H. Young, 'Computer Security Incident Response Team Effectiveness: A Needs Assessment,' *Frontiers in Psychology*, 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733042/, Last accessed: 19.04.2023.

[29] G. Killcrece, K.-P. Kossakowski, R. Ruefle and M. Zajicek, 'Organizational Models for Computer Security Incident Response Teams (CSIRTs),' Carnegie Mellon University, Software Engineering Institute, Tech. Rep., 2003. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA421684.pdf, Last accessed: 20.04.2023.

[30] International Organization for Standardization, *ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*, 2016. [Online]. Available: https://www.iso.org/standard/60803.html, Last accessed: 27.04.2023.

[31] European Union Agency for Cybersecurity, *Good practice guide for incident management*, 2010. [Online]. Available: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management, Last accessed: 11.03.2023.

[32] National Institute of Standards and Technology, 'Computer Security Incident Handling Guide,' U.S. Department of Commerce, Tech. Rep. Special Publication 800-61 Revision 2, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Last accessed: 10.03.2023.

[33] International Organization for Standardization, *ISO/IEC 27035-1:2023 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*, 2023. [Online]. Available: https://www.iso.org/standard/78973.html, Last accessed: 09.05.2023.

[34] California State University, Chico, *Evaluating Information – Applying the CRAAP Test*, 2010. [Online]. Available: https://library.csuchico.edu/sites/default/files/craap-test.pdf, Last accessed: 03.03.2023.

[35] P. Shoard, A. Davies and M. Schneider, *Magic Quadrant for Security Information and Event Management*, 2022. [Online]. Available: https://www.gartner.com/document/4019750?toggle=1&refval=361980164&ref=solrAll, Last accessed: 06.05.2023.

[36] M. Schneider, A. Davies and P. Shoard, *Critical Capabilities for Security Information and Event Management*, 2022. [Online]. Available: https://www.gartner.com/document/4021424?ref=solrAll&refval=365700177, Last accessed: 07.05.2023.

[37] Microsoft, *Microsoft sentinel data connectors*, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources, Last accessed: 10.05.2023.

[38] P. Firstbrook and C. Silva, *Magic Quadrant for Endpoint Protection Platforms*, 2022. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-2AJ91JO6&ct=220707&st=sb, Last accessed: 06.05.2023.

[39] C. Drew, E. Cordin, L. Clymer, D. Black and J. Thomas, *How Markets and Vendors Are Evaluated in Gartner Magic Quadrants*, 2020. [Online]. Available: https://www.gartner.com/document/3956304, Last accessed: 08.05.2023.

[40] National Institute of Standards and Technology, 'Guide to Cyber Threat Information Sharing,' U.S. Department of Commerce, Tech. Rep. NIST Special Publication 800-150, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf, Last accessed: 07.05.2023.

[41] J. Collins, R. Contu, M. Schneider and C. Lawson, *Market Guide for Security Threat Intelligence Products and Services*, 2021. [Online]. Available: https://www.gartner.com/document/4009281?ref=solrAll&refval=365779060, Last accessed: 09.05.2023.

[42] R. Vinot, *PyMISP Documentation*, 2023. [Online]. Available: https://buildmedia.readthedocs.org/media/pdf/pymisp/latest/pymisp.pdf, Last accessed: 12.05.2023.

[43] Microsoft, *Azure monitor agent overview*, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview, Last accessed: 12.05.2023.

[44] R. Kaur, A. Hils and T. Lintemuth, *Magic Quadrant for Network Firewalls*, 2022. [Online]. Available: https://www.gartner.com/document/4022346?toggle=1&refval=366100680&ref=solrAll, Last accessed: 06.05.2023.

[45] Palo Alto Networks, *Threat Logs*, 2023. [Online]. Available: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs, Last accessed: 12.05.2023.

[46] Microsoft, *Data collection best practices*, 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/sentinel/best-practices-data, Last accessed: 15.05.2023.

[47] R. Lee, *SIFT Workstation*. [Online]. Available: https://www.sans.org/tools/sift-workstation/, Last accessed: 13.05.2023.

[48] P. Kacherginsky, *FLARE VM: The Windows Malware Analysis Distribution You've Always Needed!* 2022. [Online]. Available: https://www.mandiant.com/resources/blog/flare-vm-the-windows-malware, Last accessed: 12.05.2023.

[49] AV-TEST, 'The AV-TEST Security Report 2019/2020,' 2020. [Online]. Available: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2019-2020.pdf, Last accessed: 09.05.2023.

[50] *Digital Forensics Artifact knowledge base*, 2023. [Online]. Available: https://artifacts-kb.readthedocs.io/_/downloads/en/latest/pdf/, Last accessed: 12.05.2023.

[51] H. van Beek, E. van Eijk, R. van Baar, M. Ugen, J. Bodde and A. Siemelink, 'Digital forensics as a service: Game on,' *Digital Investigation*, vol. 15, pp. 20–38, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287615000857, Last accessed: 14.05.2023.

[52] Hansken, *Forensic measures in Hansken*, 2021. [Online]. Available: https://www.hansken.nl/documents/publications/2021/10/01/information-document-hansken, Last accessed: 14.05.2023.

[53] Cisco, *Webex Suite eBook*, 2022. [Online]. Available: https://www.webex.com/content/dam/wbx/us/ebook/webex-suite-ebook_cm-3386.pdf, Last accessed: 16.05.2023.

[54] National Security Agency, *Selecting and Safely Using Collaboration Services for Telework - UPDATE*, 2020. [Online]. Available: https://media.defense.gov/2020/Aug/14/2002477667/-1/-1/0/CSI_%5C%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_FULL_20200814.PDF, Last accessed: 16.05.2023.

[55] H. Finney, L. Donnerhacke, J. Callas, R. L. Thayer and D. Shaw, *OpenPGP Message Format*, RFC 4880, 2007. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4880, Last accessed: 10.05.2023.

[56] Cybersecurity & Infrastructure Security Agency, *Traffic Light Protocol (TLP) Definitions and Usage*, 2022. [Online]. Available: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage, Last accessed: 11.05.2023.

[57] FIRST.org, Inc., *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0*, 2022. [Online]. Available: https://www.first.org/tlp/docs/tlp-a4.pdf, Last accessed: 11.05.2023.

[58] A. Dulaunoy, A. Iklody and S. Clement, *Best Practices in Threat Intelligence*. [Online]. Available: https://www.misp-project.org/best-practices-in-threat-intelligence.pdf, Last accessed: 11.05.2023.

[59] KnowBe4, *Assessments*. [Online]. Available: https://www.knowbe4.com/user-assessments, Last accessed: 16.05.2023.

[60] KnowBe4, *Security Awareness Training Features*, 2022. [Online]. Available: https://www.knowbe4.com/en/security-awareness-training-features/, Last accessed: 15.05.2023.

Appendix A

Standard Agreement

NTNU
Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Informasjonssikkerhet og kommunikasjonsteknologi
Veileder ved NTNU: Erjon Zoto erjon.zoto@ntnu.no 984 33 097
Ekstern virksomhet: Digitaliseringsdirektoratet Raymond Hagen Raymohag@stud.ntnu.no 926 85 771
Student: Jo Thorsen Håndstad Fødselsdato: 26.03.1999
Student: Petar Ilic Fødselsdato: 14.09.2000
Student: Sindre Logstein Fødselsdato: 17.04.1997

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 01.01.2023
Sluttdato: 22.05.2023

Oppgavens arbeidstittel er: Komponenter til å etablere et IRT-miljø

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[1]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

[1] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU: Erjon Zoto Dato: 25.01.2023
Ekstern virksomhet: Raymond Andre Hagen Raymond Andre Hagen Dato: 26.01.2023
Student: Jo Thorsen Hånstad Jo Thorsen Håndstad Dato: 17.01.2023
Student: Petar Ilic Dato: 17.01.2023
Student: Sindre Logstein Sindre Logstein Dato: 17.01.2023

Appendix B

Project Plan

NTNU

Kunnskap for en bedre verden

DEPARTMENT OF INFORMATION TECHNOLOGY AND COMMUNICATIONS TECHNOLOGY

DCSG2009

BACHELOR OF DIGITAL INFRASTRUCTURE AND CYBERSECURITY

PROJECT PLAN

Components to create an IRT environment

Jo Thorsen Håndstad, Petar Ilic and Sindre Logstein

January 2023

Contents

1. Goals and framework

1.1 Background

“Norsk offentlig sektor skal være verdensledende innen digitalisering av offentlige tjenester. Vi er godt i gang med å realisere målene for 2025 i regjeringens og KS’ digitaliseringsstrategi, men vi trenger mer kraft på arbeidet med digital sikkerhet, og vi må adressere digitalt utenforskap og brukernes tillit til offentlige digitale tjenester.” [1]

Norwegian Digitalization Agency (Norwegian: Digitaliseringsdirektoratet) is a government agency that cooperates with other government agencies with digitalization. The company employs 330 people in Oslo, Brønnøysund and Leikanger. The agency was created in 2020 when Altinn, Difi and other professional environments in Brønnøysund were merged. DIGDIR's systems run on a wide range of hardware and software. Our task will be to support these systems with components for an IRT[1].

Some of DIGDIR’s main functions are to [2]:

- Promote cooperation between government agencies.
- Development and implementation of the government's ICT (Information and Communications Technology) policy
- Strategic planning for IT infrastructure
- Information security
- Development of digital services for residents

DIGDIR must deal with environments in constant change and has therefore tasked us with researching components that can be used to protect their IT environment and systems by using an existing framework as a base. The focus will be on malware detection, surveillance and securing data in transit and in storage. The tools and solutions we find should give increased security to DIGDIR's systems.

[1] *An IRT (Incident Response Team) is a group of individuals responsible for handling and managing security incidents within an organization. An IRT can be an external entity, or an internal department separate from the IT and SOC departments in an organization.*

1.1.2 Task giver

Our task giver is Raymond Hagen. He has worked with information security for 20 years after he graduated from UiM (Norwegian: Universitetet i Molde) in Informatics. He has now begun working on a PhD through DIGDIR in "Computer and Information Systems Security." Our report will aid in his PhD, as some of the information we gather might be used in his thesis.

1.2 Project goals

1.2.1 Effect goals:

- Increase security by identifying the key components required for effective incident response in an IRT environment.
- Increasing security and streamline operations by gaining a better understanding of different IRT components.

1.2.2 Result goals:

- Make an overview of available IRT services that can help secure and support the current infrastructure.
- Mapping of DIGDIR's architecture(s) in order to find products and/or solutions that aid in increasing security in an ever more complex threat landscape.
- Make recommendations of components that should be implemented in an IRT environment in order to increase security.

1.3 Framework

1.3.1 Timeframes

- 1st of February: Project plan and standard agreement to be signed and delivered.
- 22nd of May: Delivery of the final report.

1.3.2 Other

The final report is to be written in Overleaf, a collaborative cloud-based LaTeX editor, with English as the language.

2. Scope

2.1 Problem Area

As technology is in constant development, the complexity of cyberattacks is increasing. To better secure the current infrastructure, new tools and services are needed. DIGDIR is looking to find a framework with services that can be used in incident handling and a preventive measure against cyberattacks. DIGDIR already has a repository of tools that aid in this area, but we aim to further expand this and find solutions that can be integrated with each other.

2.2 Problem delimitation

Our recommendation is based on the most reliable data we can find. We have restricted ourselves to utilizing one framework which is *FIRST CSIRT Services Framework 2.1.0* [3]. In the FIRST framework we will primarily focus on the Service Areas and find solutions based on the functions these contain. The tools we will recommend cover both hardware and software solutions. We can only find information based on publicly available documentation online and other written sources.

The project has a delivery date of 22nd of May 2023. 9 weeks will be used for research, as stated in the Gantt chart. This limits the amount of information gathering we can do. It also limits us to information available until late April 2023.

Newly developed tools with little to no information/reviews will not be considered as they will have limited information available for our research.

2.3 Problem statement

The first step will be to find the threats and adversities that a modern organization must deal with, and what kind of resources both parties might have available in attack and protection.

Our task is to find tools to recommend to an IRT that can positively influence information security event management, information security incidents management, vulnerability management, situational awareness, and knowledge transfer.

These are the main service areas outlined in FIRST, which we will focus on. The collection of tools we find should increase protection of a system's data and integrity. The tools we find

should also enhance protection on the physical layer, network layer and transport layer in the TCP/IP model.

3. Project organization

3.1 Group roles

Group leader – Petar Ilic

Secretary – Jo Thorsen Håndstad

Document manager – Sindre Logstein

3.2 Responsibilities of each role

Group leader: The most important task of the group leader is to make sure that the team's progress is in line with the relevant deadlines. Furthermore, the leader should make sure that the quality of the report and other documents meets the expectations of the task giver as well as our own.

Secretary: The task of the secretary is to write down all important information during meetings with either the task giver, student supervisor or other external parties. This will be documented in “meeting minutes” which will be uploaded to the group's OneDrive.

Document manager: The document manager should have an overview of all documents created. He should also occasionally read the documents and perform quality controls. The document manager also has the responsibility of keeping the group safe from data loss by having necessary backups.

3.3 Routines and group rules

3.3.1 Routines

- Weekly meeting with student supervisor Fridays 10:00-11:00 (subject to change).
- Weekly meeting with task giver on Fridays 11:00-12:00.
- Daily work schedule Monday-Friday 10:00-16:00. This is to ensure an estimated 30-hour work week for each person. This can vary if there are lectures or other events someone needs to attend.

3.3.2 Overview of contract

- Group members must always meet at the agreed time, unless otherwise clarified at least 12 hours before.
- Group members must be prepared for each meeting.
- Everyone should share the responsibility of the tasks.
- Help each other understand all concepts.
- Disagreements are to be solved internally, if this is not possible, it is to be taken up with the student supervisor.
- Vote on disagreements.

4. Planning, reporting and decision-making

4.1 Project framework

The framework we have decided to use for this project is the Scrum method. We feel this method fits the way we want to work with the project – in increments. Scrum also allows for people with different expertise and skills to collectively work together on one shared goal. That is why we more precisely will be using the Scrum framework known as “Expert-expert Scrum.”

Scrum is more widely used as a framework for software development. However, it has its benefits in other fields as well. And the benefits such as: improved collaboration, efficiency, flexibility, and easy to follow, manage and read progress, are the reasons we chose this framework.

A Scrum team is typically divided into roles – Product Owner, Scrum Leader, Scrum team and stakeholders. In this case the roles are as follows:

Product Owner: DIGDIR/Raymond Hagen

Scrum Leader: Jo Thorsen Håndstad

Scrum Team: Jo Thorsen Håndstad, Petar Ilic, Sindre Logstein

Stakeholders: Erjon Zoto/NTNU

Each role plays a specific and essential part in the success of the project. The Product Owner is responsible for setting the priorities and goal of the product. The Scrum Leader is responsible for facilitating the process and removing any obstacles that may arise. The Scrum team is responsible for delivering the product increment and implementing the product owner and stakeholders' requirements.

Through clearly defined roles and responsibilities, Scrum helps to ensure that everyone on the team knows what is expected of them and that the project is progressing in the right direction.

A more detailed representation of the plan will be presented with a Gantt-chart (7.1).

4.2 Plan for status meeting and decision moments in the period

Work will be done on the same document, in the same environment. This makes the status meeting redundant, but we will have a small session at the end of each day to talk about what we have accomplished and plans to move forward. We will have weekly meetings with the student supervisor and task giver (3.3.1).

Decisions will be made as a group. In cases where we are unable to come to an agreement, having a vote or contacting the student supervisor are options in order to reach a consensus.

5. Organizing of Quality Assurance

5.1 Documentation, standards, configuration

The *FIRST CSIRT Services Framework* is our main form of documentation for this project. We will consider it as the best practice in IRT operations. It will be continually used throughout the project as a tool and reference as we conduct our research and ultimately present our verdict(s).

5.2 Tools

Table 1: Tools

Name:	**Type:**	**Area of use:**
Teams	Communication and file sharing	Teams will be used to communicate and share files with the task giver and student supervisor.
Overleaf	LaTeX editor	A cloud-based editor that allows us to author the final report in collaboration
OneDrive	Cloud-based file sharing platform	File storage and sharing
Office	Collaboration	Cloud based productivity platform mainly used for time sheets, meeting minutes etc.
Discord	Communication platform	Internal communication with group members

5.3 Plan for inspection and testing.

We will have to rely on third party testers with the tools we will recommend. This can be user reviews or related documentation. Testing is important since the information from the producer might be unreliable or presented in an overly positive manner to increase the sales. We do not have the facilities nor the budget to conduct our own testing, this makes us rely on publicly available information. We will therefore strive to find multiple independent sources for a tool and will not recommend one if the information is contradictory or limited.

6. Risk analysis

6.1 Identify and analyze risk

In the table below, we identify risks that are involved with this project and events that could

negatively impact our project work. The table show the likelihood, impact, priority and if we have a plan for managing the risk. The likelihood and impact will be on a scale from low to high. Priority is based on the likelihood and impact.

Table 2: Risk identification

Risk	Likelihood	Impact	Priority	Action
Lack of participation or commitment from group members	Low	High	High	Yes
Difficulty in coordinating schedules and meeting deadlines	Medium	High	High	Yes
Inadequate communication and poor teamwork	Low	High	Medium	Yes
Different working styles or conflicting ideas leading to disagreements	Medium	High	High	No
Inability to effectively divide and delegate tasks	Medium	Medium	Medium	Yes
Risk of group members not contributing equally to the project	Medium	High	High	Yes
Risk of group members not having the necessary skills or knowledge to complete the project	Medium	High	High	No
Risk of illness	Low	Medium	Low	No
Risk of data loss	Low	High	High	Yes
Risk of inadequate research	Medium	Medium	Medium	Yes

6.2 Plan for managing the risk

Below is a table that describes what measures we can take to manage the risks. The measures either lower the likelihood or the impact of the risks.

Table 3: Risk management

Risk	Prevention Measures
Lack of participation or commitment from group members	Clearly define roles and expectations for group members. Establish regular check-ins and progress updates. Encourage open communication and active participation.
Difficulty in coordinating schedules and meeting deadlines	Create a detailed project plan and schedule with specific deadlines, mainly using a Gantt-chart.
Inadequate communication and poor teamwork	Encourage open and regular communication among group members. Establish clear channels for communication (e.g., Microsoft Teams), while working together on campus is always the priority.
Inability to effectively divide and delegate tasks	Clearly defining roles and the expectations of these roles.
Risk of group members not contributing equally to the project	All group members, while keeping to their roles, should somewhat contribute to all parts of the project, to get an understanding of the project altogether.
Risk of data loss	We will have backups online as well as store information locally on our computers. This makes it so information is stored in a minimum of 4 places. The main report will be stored in Overleaf with git as the version control, which will be pulled to our shared OneDrive.
Risk of inadequate research	Make suitable time for research and effective use of our task giver's knowledge and expertise as we are conducting our research.

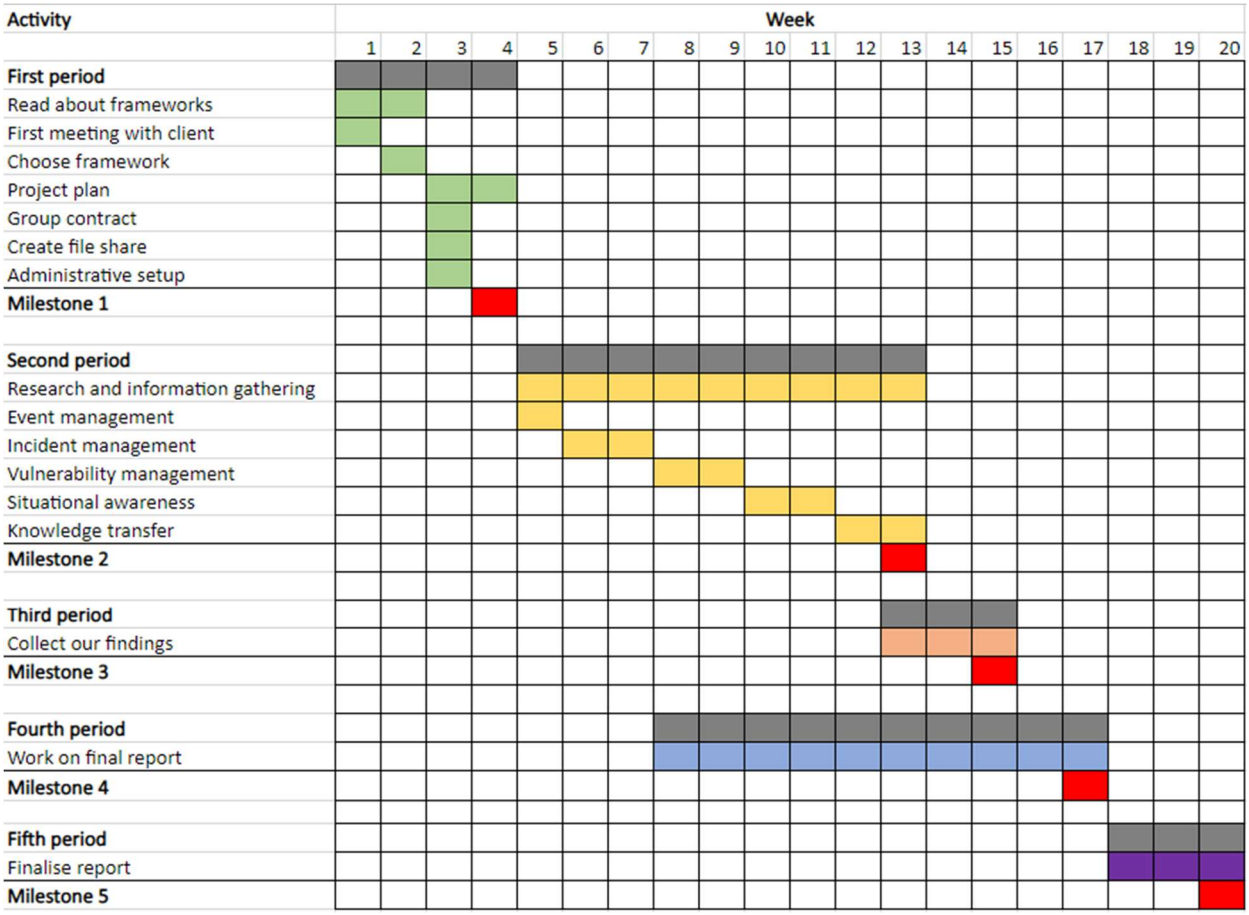
7. Scrum plan and Gantt-chart

7.1 Scrum plan

Table 5: Scrum plan

Period	Sprints	Length of sprint	Length of period
Planning and strategy	2	1-2 weeks	4 weeks
Research	5	1-2 weeks	9 weeks
Collect and sort findings	1	3 weeks	3 weeks
Work on final report	3	2-6 weeks	10 weeks
Finalise final report	1	3 weeks	3 weeks

7.2 Gantt-chart



8. Bibliography

1. Digitaliseringsdirektoratet. (n.d.). *Rikets digitale tilstand*. Available at: https://www.digdir.no/rikets-digitale-tilstand/rikets-digitale-tilstand/3480 (Accessed: 23.01.2023).

2. Digitaliseringsdirektoratet. (n.d.). *Kva er Digitaliseringsdirektoratet?* Available at: https://www.digdir.no/digdir/kva-er-digitaliseringsdirektoratet/703 (Accessed: 23.01.2023).

3. FIRST.org, Inc. (2019). *Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0*. Available at: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf (Accessed 23.01.2023).

Appendix C

Gantt Chart

Activity	Week																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
First period																				
Read about frameworks																				
First meeting with client																				
Choose framework																				
Project plan																				
Group contract																				
Create file share																				
Administrative setup																				
Milestone 1																				
Second period																				
Research and information gathering																				
Event management																				
Incident management																				
Vulnerability management																				
Situational awareness																				
Knowledge transfer																				
Milestone 2																				
Third period																				
Collect our findings																				
Milestone 3																				
Fourth period																				
Work on final report																				
Milestone 4																				
Fifth period																				
Finalise report																				
Milestone 5																				

Appendix D

Task Description

Komponenter til å etablere et IRT miljø?

Jeg tar en Off. PHD gjennom Digitaliseringsdirektoratet, som har tjenester for dialog mellom organisasjoner, virksomheter og individ med det offentlige. De mest kjente tjenestene som Digitaliseringsdirektoratet tilbyr er Altinn og id-porten. I tillegg til 20 andre offentlig IKT løsninger.

Løsningene er basert på ulike driftsmodeller. Noe er håndtert «on premise», det betyr at de er driftet hos en lokal driftsleverandør i Norge. Noen er driftet i skytjenestene Microsoft Azure og Google Cloud services. Det er heterogenene systemer som baserer seg på Windows, Linux .NET Core, og Kubernetes blant annet.

Oppgaven

Det kommer stadig flere nye løsninger til i miljøet vårt, og Vi ønsker å bruker produkter som understøtter en god sikkerhetsarkitektur. Ønsket er at det gjøres en litteraturstudie som tar utgangspunkt i et rammeverk. Eksempel kan være CERT konseptet fra CMU (Carnigie Mellon University), eller FIRST rammeverket for hendelseshåndtering. Det finnes flere andre også.

Etter at dere har funnet et rammeverk for sikker oppbygging av de ulike typene nettverk, så ønskes det at dere ser på teknologier som understøtter de ulike arkitekturene. Fokus vil være skadevaredeteksjon, overvåking, sikring av data både under transport og i lagring. Og foreslåtte løsninger må prøve å gi en totalbeskyttelse på både fysisk, nettverk, transport og applikasjonslaget (ref TCP / IP) modellen.

Oppgavens mål

Oppgavens mål er å få oversikt over hvilke produkter og løsninger som finnes for cyber sikkerhet. Det er veldig mange leverandører, og det er et veldig stort antall ulike sårbarheter og trusler. Litteraturstudien vil være å systematisk gå gjennom de forskjellige arkitekturene som DigDIR har, og se etter produkter ,eller løsninger som kan håndtere et stadig mer komplekst trusselbilde. Oppgaven skal være en litteraturstudie, og dertil analyse.

Oppgavens krav

- Forstå de ulike tekniske løsningene som DigDIR
- Forstå angrepsflater og sårbarheter
- Kunne gjennomføre trusselmodellering og risikoanalyse
- Finne frem til ulike produkter, gjerne gjøre sammenligninger basert på åpen informasjon, og gi en anbefaling for at nettverket med tilhørende applikasjoner blir sikret på et tilfredsstillende vis.

- Estimere hva som vil kreves av prosesser og mennesker for å kunne beskytte et system tilstrekkelig.

Det vil ikke være en fasit, for en slik oppgave, men siden vi har en del forskjellige løsninger med tilhørende arkitektur, så forventes det at det vil være utfordrende å finne løsninger og produkter som går på tvers av de ulike løsningene. Det vil i tillegg være naturlig at dere gjør dere opp en vurdering om produkter kan gjøre alt de lover. For eksempel AI baserte anti malware løsninger.

Ønsket er at dere bruker tid på å sette dere inn i problemstillingen, og siden jeg skriver på en PHD om statsfinansierte avanserte trussel aktører, at jeg kan hente inspirasjon fra arbeidet deres.

Raymond Andre Hagen

raymohag@stud.ntnu.no / raymond.andre.hagen@digdir.no

Appendix E

National Cyber Security Center (NCSC) – Expert Interview

Kan du fortelle litt om deg selv? (Rolle, bakgrunn, ansvarsområder i NCSC)

Navn: Reidar Mouhleb

Jobbet i NSM i 8 år som informatiker, samt kvalitetsordning og partnerkontakt.

Hvilke verktøy og teknikker bruker dere for å oppdage og respondere til sikkerhetshendelser?

Noe er GRADERT og ikke med her. Enkelte deler er egenutviklet, men i stort er det forskjellige kommersielle løsninger som benyttes.

Hvilke monitoreringsverktøy bruker dere? (SIEM, sensorer etc.)

Noe er GRADERT og ikke med her, men også her er det en stor andel kommersielt tilgjengelige verktøy.

Hvilke ulike komponenter benytter VDI? For eksempel hvilke nettverkssensorer?

For det meste GRADERT informasjon. Men VDI består av sensorer plassert hos partnere. Sensorer trenger "ferskvare" i form av signaturer etc., så hva man fyller sensorer med er viktig for å innhente ønsket data.

Hvordan ser deres hendelsesresponsprosess ut fra deteksjon til løsning?

- Når en hendelse inntreffer er det den berørte virksomheten som eier hendelsen. Det vil si at de bestemmer hvor mye og hvilken informasjon som skal deles om hendelsen til andre virksomheter/SRM/offentligheten.

– NCSC gir råd og/eller støtte under hendelser, henviser til andre IRT virksomheter, for eksempel de vi har godkjent i kvalitetsordningen eller andre, dersom en hendelse ikke er alvorlig nok for NCSC.

Hvordan kommuniserer dere med klienter? (Under vanlige forhold og krisesituasjoner)

Kommunikasjon skjer etter avtale og hva som er hensiktsmessig. Gjerne gjennom Teams dersom det er snakk om ugradert informasjonsdeling. For gradert informasjon benyttes fysiske møter eller dertil egnede plattformer.

Hvordan utfører dere deteksjon og hvordan samler dere denne dataen?

Sensorer – ytterligere informasjon om disse er GRADERT.

I hvor stor grad benytter dere automasjon og evt. AI i deres løsninger?

Ikke modent nok.

Bruker dere out-of-the-box løsninger eller utvikler dere verktøy selv?

GRADERT, men en stor andel kommersielt tilgjengelige verktøy.

Hva er de største utfordringene til dagens SRM-løsninger?

En SRM-løsning er ikke for alle. Størrelsen på en SRM er en viktig faktor i å avgjøre om de møter kravene til en sektor. Digdir kan muligens passe som SRM ift. størrelse. Et stort pluss er samarbeidet det skaper imellom SRM-er, virksomheter og myndigheter.

Hva kreves for å være medlem av FIRST?

For å bli medlem av FIRST må man bli anbefalt av andre FIRST-medlemmer (to sponsorer). Se First sine nettsider: Becoming a Member (first.org).

Appendix F

Table of All Components and Associated Roles

FIRST Services and Functions	Proposed Components	Alternative Components	Associated Roles
Infromation Security Event Management			
Monitoring and detection			
Log and sensor management	Microsoft System Center Configuration Manager	Red Hat Ansible	System and Sensor Administrator
	Microsoft System Center Operations Manager	Nagios XI	
	Palo Alto NGFW	FortiGate NGFW, Cisco FirePower	
	Snort	ManageEngine Log360, SolarWinds SEM	
Detection use case managemnet	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Use Case Manager
Contextual data management			Data Manager
Event analysis			
Correlation	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Incident Analyst
Qualification			Incident Triage Coordinator
Infromation Security Incident Management			
Information security incident report acceptance			
Information security incident report receipt	Cisco Webex	LINK Mobility, Slack, Wire	Incident Triage Coordinator
	PGP (Pretty Good Privacy / TLP (Traffic Light Protocol)		
Information security incident triage and processing	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	
	MISP (Malware Information Sharing Platform)	CrowdStrike Falcon Intelligence, AT&T AlienVault OTX, IBM X-Force Exchange	
Information security incident analysis			
Information security incident triage (prioritization and categorization)	Microsoft 365 Defender	CrowdStrike Falcon Insider, Palo Alto Cortex	Incident Triage Coordinator
	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	
Information collection	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Incident Responder
	Palo Alto NGFW	FortiGate NGFW, Cisco FirePower	
	Snort	ManageEngine Log360, SolarWinds SEM	
	Microsoft 365 Defender	CrowdStrike Falcon Insider, Palo Alto Cortex	
Detailed analysis coordination	Cisco Webex	LINK Mobility, Slack, Wire	
	Bestpractical RTIR (Request Tracker for Incident Response)		
Information security incident root cause analysis	Employee		Incident Analyst

Cross-incident correlation	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Incident Analyst, Malware / Forensic Analyst
Artifact and forensic evidence analysis			
Media or surface analysis	Hansken		Incident Analyst, Malware / Forensic Analyst
	Artefact-kb		
	RSS (Really Simple Syndication)		
Reverse engineering	SIFT		Malware / Forensic Analyst
	FLARE VM		
Run time or dynamic analysis	SIFT		
	FLARE VM		
Comparative analysis	Hansken		
	Artefact-kb		
Mitigation and recovery			
Response plan establishment	Employee		Incident Responder
Ad hoc measures and containment	Microsoft 365 Defender	CrowdStrike Falcon Insider, Palo Alto Cortex	
System restoration	Micrososft System Center Operations Manager	Nagios XI	IT Administrator
Other information security entities support	Employee		Incident Responder
Information security incident coordination			
Communication	Cisco Webex	LINK Mobility, Slack, Wire	Incident Responder
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
Notification distribution	Cisco Webex	LINK Mobility, Slack, Wire	
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
Relevant information distribution	Cisco Webex	LINK Mobility, Slack, Wire	
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
Activities coordination	Cisco Webex	LINK Mobility, Slack, Wire	
	Bestpractical RTIR (Request Tracker for Incident Response)		
Reporting	Cisco Webex	LINK Mobility, Slack, Wire	
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
	Bestpractical RTIR (Request Tracker for Incident Response)		
Media communication	Employee		Communication Liaison

Crisis management support			
Information distribution to constituents	Cisco Webex	LINK Mobility, Slack, Wire	Communication Liaison
Information security status reporting	Cisco Webex	LINK Mobility, Slack, Wire	Incident Triage Coordinator
	Bestpractical RTIR (Request Tracker for Incident Response)		
Strategic decisions communication	Cisco Webex	LINK Mobility, Slack, Wire	Communication Liaison
Vulnerability Management			
Vulnerability discovery / research			
Incident response vulnerability discovery	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Incident Analyst, Malware / Forensic Analyst
Public source vulnerability discovery	NVD (National Vulnerability Database)		Vulnerability Analyst
	CVE (Common Vulnerabilities and Exposures)		
Vulnerability research	Tenable Nessus	CrowdStrike Falcon Spotlight, Microsoft Defender Vulnerability Management	Vulnerability Researcher
	FLARE VM		
Vulnerability report intake			
Vulnerability report receipt	Cisco Webex	LINK Mobility, Slack, Wire	Vulnerability Triage Coordinator
Vulnerability report triage and processing	Tenable Nessus	CrowdStrike Falcon Spotlight, Microsoft Defender Vulnerability Management	
	Rapid7 InsightVM		
Vulnerability analysis			
Vulnerability triage (validation and categorization)	EPSS (Exploit Prediction Scoring System)		Vulnerability Triage Coordinator
Vulnerability root cause analysis	Employee		Vulnerability Analyst
Vulnerability remediation development			
Vulnerability coordination			
Vulnerability notification/reporting	Cisco Webex	LINK Mobility, Slack, Wire	Vulnerability Coordinator
Vulnerability stakeholder coordination			
Vulnerability disclosure			
Vulnerability disclosure policy and infrastructure maintenance	TLP (Traffic Light Protocol)		Vulnerability Disclosure Coordinator
Vulnerability announcement/ communication/dissemination	Cisco Webex	LINK Mobility, Slack, Wire	
Post-vulnerability disclosure feedback			

Vulnerability response			
Vulnerability detection / scanning	Tenable Nessus	CrowdStrike Falcon Spotlight, Microsoft Defender Vulnerability Management	Vulnerability Assessment Analyst
	Rapid7 InsightVM		
Vulnerability remediation	Tenable Nessus		IT Security Administrator
	Rapid7 InsightVM		
Situational Awareness			
Data acquisition			
Policy aggregation, distillation, and guidance	Employee		Situational Awareness Manager
Asset mapping to functions, roles, actions, and key risks	Microsoft System Center Operations Manager	Nagios XI	Risk & Continuity Advisor / Risk Analyst
Collection	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Situational Awareness Data Analyst
	RSS (Really Simple Syndication)		
Data processing and preparation	Employee		
Analysis and synthesis			
Projection and inference	Employee		Situational Awareness Data Analyst
Event detection (through alerting and/or hunting)	Microsoft Sentinel	Splunk, IBM QRadar, LogRythm	Threat Warning Analyst
	MISP (Malware Information Sharing Platform)	CrowdStrike Falcon Intelligence, AT&T AlienVault OTX, IBM X-Force Exchange	
Information security incident management decision support	Employee		
Situational impact			
Communication			
Internal and external communication	Cisco Webex	LINK Mobility, Slack, Wire	Threat Warning Analyst
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
Reporting and recommendations	Employee		
Implementation			
Dissemination / integration / information sharing	Cisco Webex	LINK Mobility, Slack, Wire	Communication Liaison
	PGP (Pretty Good Privacy) / TLP (Traffic Light Protocol)		
Management of information sharing	Cisco Webex	LINK Mobility, Slack, Wire	
	MISP (Malware Information Sharing Platform)	CrowdStrike Falcon Intelligence, AT&T AlienVault OTX, IBM X-Force Exchange	
Feedback	Cisco Webex	LINK Mobility, Slack, Wire	

Knowledge Transfer			
Awareness building			
Research and information aggregation	KnowBe4	Microsoft Forms, Articulate 360, Sophos	Awareness Coordinator
	MISP (Malware Information Sharing Platform)	CrowdStrike Falcon Intelligence, AT&T AlienVault OTX, IBM X-Force Exchange	
	NSM basic principles for ICT Security		
	NCI (National council of ISACs)		
Reports and awareness materials development	KnowBe4	Microsoft Forms, Articulate 360, Sophos	
Information dissemination	RSS (Really Simple Syndication)		
Outreach	MISP (Malware Information Sharing Platform)	CrowdStrike Falcon Intelligence, AT&T AlienVault OTX, IBM X-Force Exchange	
	NCI (National council of ISACs)		
Training and education			
Knowledge, skill, and ability requirements gathering	KnowBe4	Microsoft Forms, Articulate 360, Sophos	Training Developer
Educational and training materials development			
Content delivery			
Mentoring	MentorCloud		Staff Developer
CSIRT staff professional development	Certifications		
	Events(Infosecurity Europe, RSA Conference, SANS)		
	MentorCloud		
Exercises			
Requirements analysis	KnowBe4	Microsoft Forms, Articulate 360, Sophos	Training Developer
Format and environment development			
Scenario development			
Exercise execution			
Exercise outcome review			
Technical and policy advisory			
Risk management support	Employee		Risk & Continuity Advisor / Risk Analyst
Business continuity and disaster recovery planning support			
Policy support			Policy Advisor
Technical advice			Technical Policy Advisor

Appendix G

Service Areas, Services and Functions of the FIRST CSIRT Services Framework


SERVICE AREA
Information Security Event Management
Monitoring and Detection
• Log and Sensor Management
• Detection Use Case Management
• Contextual Data Management
Event Analysis
• Correlation
• Qualification
SERVICE AREA
Information Security Incident Management
Information Security Incident Report Acceptance
• Information Security Incident Report Receipt
• Information Security Incident Triage and Processing
Information Security Incident Analysis
• Information Security Incident Triage (Prioritization and Categorization)
• Information Collection
• Detailed Analysis Coordination
• Information Security Incident Root Cause Analysis
• Cross-Incident Correlation
Artifact and Forensic Evidence Analysis
• Media or Surface Analysis
• Reverse Engineering
• Runtime or Dynamic Analysis
• Comparative Analysis
Mitigation and Recovery
• Response Plan Establishment
• Ad Hoc Measures and Containment
• System Restoration
• Other Information Security Entities Support
Information Security Incident Coordination
• Communication
• Notification Distribution
• Relevant Information Distribution
• Activities Coordination
• Reporting
• Media Communication
Crisis Management Support
• Information Distribution to Constituents
• Information Security Status Reporting
• Strategic Decisions Communication
SERVICE AREA
Vulnerability Management
Vulnerability Discovery/Research
• Incident Response Vulnerability Discovery
• Public Source Vulnerability Discovery
• Vulnerability Research
Vulnerability Report Intake
• Vulnerability Report Receipt
• Vulnerability Report Triage and Processing
Vulnerability Analysis
• Vulnerability Triage (Validation and Categorization)
• Vulnerability Root Cause Analysis
• Vulnerability Remediation Development
Vulnerability Coordination
• Vulnerability Notification/Reporting
• Vulnerability Stakeholder Coordination
Vulnerability Disclosure
• Vulnerability Disclosure Policy and Infrastructure Maintenance
• Vulnerability Announcement/ Communication/Dissemination
• Post-Vulnerability Disclosure Feedback
Vulnerability Response
• Vulnerability Detection/Scanning
• Vulnerability Remediation
SERVICE AREA
Situational Awareness
Data Acquisition
• Policy Aggregation, Distillation, and Guidance
• Asset Mapping to Functions, Roles, Actions, and Key Risks
• Collection
• Data Processing and Preparation
Analysis and Synthesize
• Projection and Inference
• Event Detection (through Alerting and/or Hunting)
• Situational Impact
Communication
• Internal and External Communication
• Reporting and Recommendations
• Implementation
SERVICE AREA
Knowledge Transfer
Awareness Building
• Research and Information Aggregation
• Report and Awareness Materials Development
• Information Dissemination
• Outreach
Training and Education
• Knowledge, Skill, and Ability Requirements Gathering
• Educational and Training Materials Development
• Content Delivery
• Mentoring
• CSIRT Staff Professional Development
Exercises
• Requirements Analysis
• Format and Environment Development
• Scenario Development
• Exercise Execution
• Exercise Outcome Review
Technical and Policy Advisory
• Risk Management Support
• Business Continuity and Disaster Recovery Planning Support
• Policy Support
• Technical Advice

Appendix H

Meeting Minutes With Task Giver

05.01.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 1 hours

What we discussed:

We had a first meeting with the client and got an overview of the project and what tasks we should do for our next meeting.

He showed us some recourses that we should go through for the next meeting

13.01.2023

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 1 hours

What we discussed:

During the meeting we discussed the contract. We then talked about frameworks such ISO 27000 and FIRST and how for the creation of an CSIRT, FIRST is better.

Lastly the layout of the task was discussed and the optimal distribution of content in each chapter was intro 10%, dicussion 80% and outro 10%.

20.01.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 1 hours

What we discussed:

First, we concluded that both software and hardware should be discussed in the solution.

Hardware needs the capability to support zones, encryption, firewall and support a forensics toolbox. Software such as IDS, passive DNS, HIDS was also discussed.

Our solution should support already existing infrastructure and offer value when things get hard. The CSIRT should be its own unit separate from Digdir

27.01.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

Digdir has both infrastructure on premises and in the cloud but mainly in the cloud. If we choose cloud in our solution it needs to be hosted in a NATO country.

A CSIRT is not an alternative to an IT department or a SOC as an CSIRT is reactive and is only called upon if things have gone dreadfully wrong.

Many of the tools we recommend will need specialists to maintain.

03.02.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The development of infrastructure at Digdir is positive for the solution and the CSIRT need a separate unit to do forensics.

We need to have a diagram that shows where we gather data from.

A SIEM solution is hard as correlation of data get complicated when there are logs from different systems including Windows and Linux. A SIEM might collect up to 100GB of data in a day and the it makes correlation important to reduce its complexity.

10.02.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The meeting with NCSC might not result in much usable information but Raymond will get us the architecture over the different departments at Digdir.

What are the benefits and drawbacks of having filtering at the constituencies and we should describe both alternatives.

Make a drawing of the architecture needed where SIEM is the backbone.

17.02.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

Will have a physical meeting with Raymond at 14:40 21.02.

Don’t recommend products which are unsupported as it's hard to patch it. It is important that the producer is still supporting it with regular updates.

Having an XDR and using Hansken is good tools for the creation of a CSIRT.

The solution should say something about what tools are needed to comply with the FIRST framework.

Where should filtering take place?

How to classify an attack, remote or local, what vulnerability is being used and how hard is it to protect against.

03.03.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The procedures at NSM and what is important that we get from the tour.

How much and what data does a CISRT need and what are the different services that can be offered. What might be a solution if one of the constituency's doesn't want to give away data.

17.03.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The meeting with NCSC won't happen before April.

The solution don’t need to monitor the constituency's like in a SOC but it should protect them. The solution should include information gathering, advice, situational awareness.

The discussion should have a section to assess whether the product possesses functionalities that do not align with the established concept. These functionalities may be inherent to the vendor's solution, it is crucial to evaluate whether they truly enhance the overall solution or contribute to unnecessary complexity. More tools and components will also lead to a bigger risk for misconfiguration.

An estimated cost analysis should be done and how many people is needed for the operations of every component.

A total situational awareness picture should be created and a discussion on what justifies the creation of a SOC and an CSIRT.

Long neck paradox that states that the threats most relevant to the constituency's are old ones as many organizations don’t have time to implement new technology into their infrastructure such as using blockchain.

31.03.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

NCSC is there to see the overall picture on security in Norway, but they can't see everything. There is therefore also the need for SRMs that are responsible for security in different sectors.

The SRMs can share information between each other and with NorCERT that can share to other SRMs.

There is no CERT in Norway yet for every sector.

The main part of the task is to find technology's that can support the functions of the FIRST framework.

There are benefits to have an overall overview over the products a constituency possesses as it is easier in helping them get situational awareness.

14.04.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The objective of a CSIRT and its main selling point is that it can provide a fast way for an organization to restore normal operation. The SOCs responsibility is to do incident response. Another main function for a CSIRT is to do situational awareness and communication. One of the main goals of a CSIRT is to gain complete situational awareness. The sharing of data is also an important aspect.

Remove sentences from the report that doesn't provide information. Start every paragraph right on.

What do we think about a CSIRT. Is it necessary, does it enhance security, is it to much work to establish, should Digdir have one for every department or should it be one common.

21.04.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 120 minutes

What we discussed:

Important to include how many people are needed to support a CSIRTs operations and what expertise they need to possess. Estimating cost will be speculative.

Write the report in parts: the architecture, the service area, The CSIRTs infrastructure, this support different capabilities and this is a sensor in the clients infrastructure.

Ninja is a Linux with premade functions for forensics

How much support should a CSIRT give for system restoration if any. The CSIRTs role is not to manage a backup solution but rather give support to restore the operations. During an attack the CSIRT should do mitigation actions.

A CSIRT should have a web solution to give advice and ease communication.

The report should show that every technology is reliant on each other, and they don't exist in a vacuum.

A CSIRT can give its client confidence in its security by giving advice on what should change for it to improve.

The task has become more and more about describing the solution with the different tools. Every tool should be thoroughly described including how they work together and how they are used in practice.

It is important that the report shows how complex the solution is. This complexity arises from the multitude of tools required, all of which must seamlessly integrate and collaborate. Moreover, many of these tools are intricate in nature and rely on the support of other tools to function optimally.

28.04.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The meeting with NCSC and what we needed to have with us to be allowed in.

The government has enough money to pay for most solutions as a security breach will lead to large expenses.

The solution should be presented as early as possible to give the reader an overview. The report doesn't need to show that we have understood the capabilities of each tool completely, but it should be enough to sell it to the reader as a capable tool. A picture for each tool is also recommended.

05.05.2023

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Raymond Hagen

Time: 60 minutes

What we discussed:

The meeting with NCSC went well. The solution we are creating, and NCSC solution is different because complying with every function in the FIRST framework is too complex for an organization to do.

There should be a chapter that talk about future work. For example, talk about some solutions that NCSC have that we don't have time to implement.

The tools should be visualized and then explained.

The XDR could either be the constituencies or the CSIRTs responsibility but responding to attacks are not the CSIRTs responsibility.

Appendix I

Meeting Minutes With Supervisor

17.01.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 1 hours

What we discussed:
Erjon's office is at T-516 5th floor in the Topas building.

27.01.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 30 minutes

What we discussed:

Add title to project plan

Add more limitations – online sources, sources related to this point in time

It would be nice to mention a list of possible frameworks to choose from in the final report and say that among these the FIRST was more suitable.

The IRT specifically for DIGDIR

Mention typical components for an IRT and then suggest relevant components to DIGDIR

First draft of report should be delivered around April

Image showing how the Scrum process will work(?)

02.02.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 30 minutes

What we discussed:

Meeting with Erjon should be held at 10 every Friday

The phases in the Gant chart should be named

The report should describe the task and the way we worked while the conclusion should describe what went wrong.

What is the most appropriate framework and what are its limitations compared to others?

Erjon will help us get into contact with master student and it may be beneficial to read his report.

Recommend tools that can fit well with Digdir and not the tools in the best case scenario.

Some good news sites are TechTarget and ComputerWeekly,

03.03.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 30 minutes

What we discussed:

Use templates with affiliation to NTNU in overleaf but focus on writing for now.

The IMRAD model should be fine to use for research. FIRST framework should be in the methodology.

Finished with the Service area 1 in the FIRST framework and will start on service area 2. Some parts of Service area 2 has already been addressed by tools found in service area 1.

10.03.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein, Raymond Hagen and Erjon Zoto

Time: 60 minutes

What we discussed:

We showed Raymond our Overleaf and discussed what chapters would be needed.

Raymond gave us some pointers on the theory chapter so that it was easier for the reader to understand. Every thing should also be built up to the framework and discussing APTs would make it easier for the reader to understand the importance of a CSIRT.

The methodology should have sections about where we got the theory from and explain the sources we used. It should also emphasize that we have conducted a thorough literature review and that the task is based on a solid theoretical framework to derive practical solutions.

The next chapter should document the components. A table should be used that includes the service area, component type, relevant products, and a brief description of each product.

The thesis should have both a conclusion and a discussion chapter.

A discussion on the need for each service area might be good to include with sections about why the service is needed what components we choose for each and how to gather the data for each component. It should also include the best way to send the data to the component.

Another section should discuss if we finished what the task asked of us.

14.04.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 30 minutes

What we discussed:

A draft of the report should be delivered on 17 of April to get feedback from Erjon on the structure and what we have done so far.

Interview with NCSC should be in methodology as well as sources and the FIRST framework.

Informal interviews should be included in the report if they are relevant and can provide valuable insights or additional information to enhance the understanding or analysis of the subject matter.

The report should be written in a manner that ensures comprehensibility for non-technical individuals who may not possess an IT background.

27.04.23

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 60 minutes

What we discussed:

The comments from Erjon on the first draft of the report was discussed.

The recherché phase is done and the plan forward is to write the result part of the report. The way we want to present it is to describe the tools and describe how they fulfil the functions in the FIRST framework.

A new version will be sent to Erjon next week.

There is a need to write the text more formal.

Add human aspect in theory that describes how to use each tool efficiently and used in the right way.

Methodology should have a chapter on what words we used when we tried to find information about each tool.

The interview with NCSC should be documented thoroughly and we need to prepare some questions in preparation for the meeting.

05.05.2023

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 60 minutes

What we discussed:

Erjon had some comment on the second draft of the report including: Adding explanations for the colours in the table in the methodology.

Tabels should be used where it is possible instead of using figures.

The report needs to have more about how we found our sources.

The meeting with NSCS was important to include in the report in some way

16.05.2023

Participants

Petar Ilic, Jo Thorsen Håndstad, Sindre Logstein and Erjon Zoto

Time: 60 minutes

What we discussed:

The report needs to define Digdir and an image need to be added to explain Mitre

There should be more written about the human aspect for the solution.

Some content can be changed to the theory section of the report.

The report should have discussion and conclusion and include what could have been done differently. It also needs to include future work.

The FIRST framework should not be included in the Appendix.

Appendix J

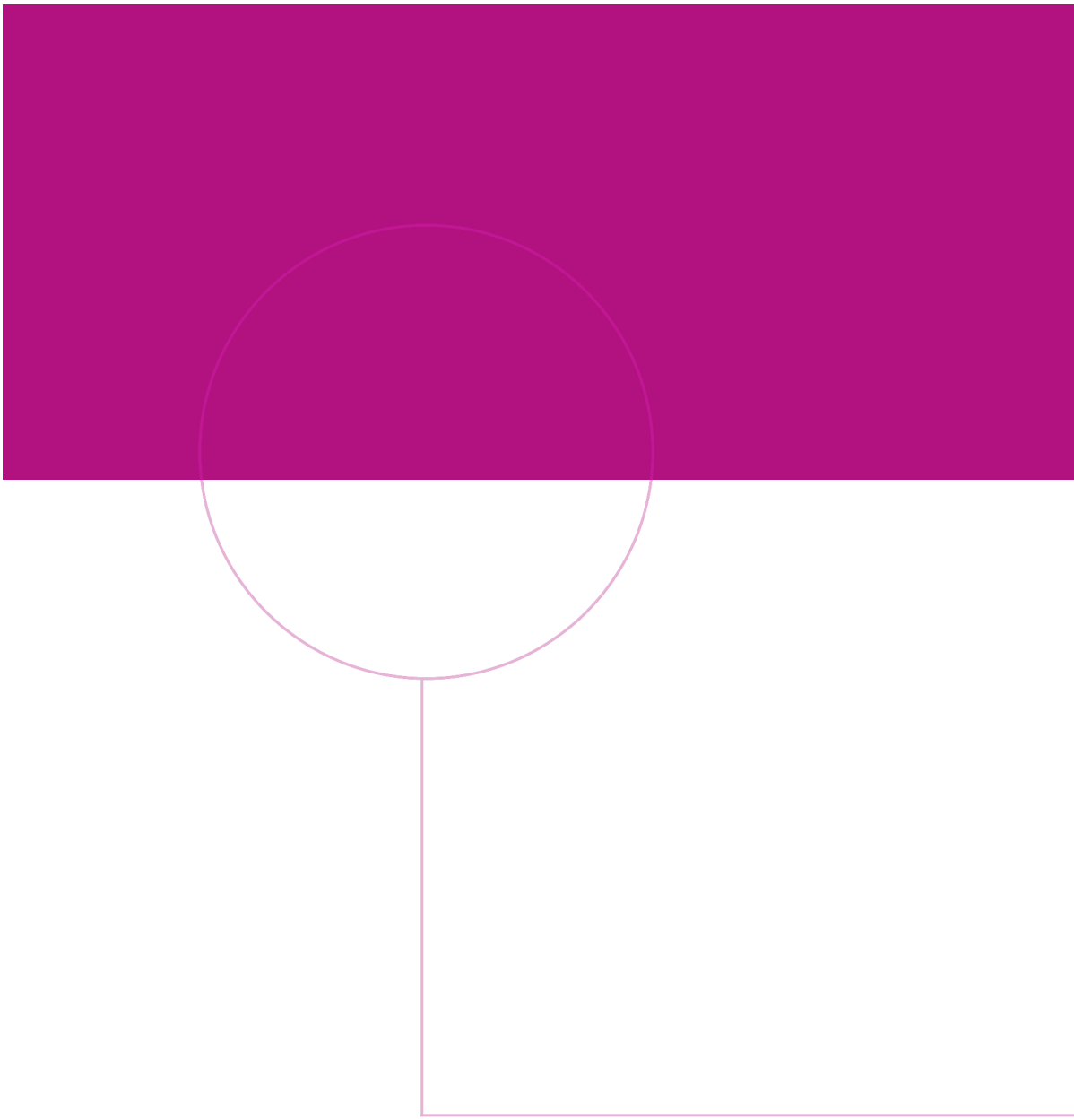
Timesheet

Date	Petar		Sindre		Jo	
	Activity	Hours	Activity	Hours	Activity	Hours
05.01.23	Meet and greet with client	1	Meet and greet with client	1	Meet and greet with client	1
06.01.23					Read through First framework 1.1	1
11.01.23	Lynkurs 1 - Prosjektstyring	2	Lynkurs 1 - Prosjektstyring	2	Lynkurs 1 - Prosjektstyring	2
12.01.23	Setup of basic administrative resources	3	Setup of basic administrative resources	3	Setup of basic administrative resources	3
13.01.23	Meeting with client	1	Meeting with client	1	Meeting with client	1
16.01.23	Started writing the project plan	4	Started writing the project plan	4	Started writing the project plan	4
17.01.23	Continuing the project plan	5	Continuing the project plan	5	Continuing the project plan	5
17.01.23	Meeting with coordinator	0.5	Meeting with coordinator	0.5	Meeting with coordinator	0.5
18.01.23	Guest lecture "Det var en gang et cyberangrep", Sopra Steria	2	Guest lecture "Det var en gang et cyberangrep", Sopra Steria	2	Guest lecture "Det var en gang et cyberangrep", Sopra Steria	2
18.01.23	Further work with the project plan	4	Further work with the project plan	4	Further work with the project plan	4
19.01.23	Further work with the project plan	3	Further work with the project plan	3	Further work with the project plan	3
20.01.23	Meeting with client	1	Meeting with client	1	Meeting with client	1
23.01.23	Finalising project plan	4	Finalising project plan	4	Finalising project plan	4
24.01.23	Read the entirety of the FIRST framework	2.5	Read Service Area 5 or the FIRST framework	0.5	Read Service Area 5 of the FIRST framework	0.5
24.01.23	Research - SA1	4	Research - SA1	4	Research - SA1	4
25.01.23	Research - SA1	4	Research - SA1	4	Research - SA1	4
26.01.23	Meeting with client and project supervisor	1.5	Meeting with client and project supervisor	1.5	Meeting with client and project supervisor	1.5
26.01.23	Project plan	5	Project plan	5	Project plan	5
30.01.23	Finishing project plan	3	Finishing project plan	3	Finishing project plan	3
31.01.23	Research and worked on LaTeX environment	4	Research	4	Research siem (splunk,at&t, gartner)	4
01.02.23	Research	4	Research	4	Research	4
02.02.23	Meeting with coordinator - research after	3	Meeting with coordinator - research after	3	Meeting with coordinator - research after	3
03.02.23	Meeting with task giver	1	Meeting with task giver	1	Meeting with task giver	1
06.02.23	Research - SA1	4	Research - SA1	4	Research - SA1	4
07.02.23	Research - SA1	4	Research - SA1	4	Research - SA1	4
10.02.23	Research - SA1, Meeting with client and supervisor	4	Research - SA1, Meeting with client and supervisor	4	Research - SA1, Meeting with client and supervisor	4
13.02.23	Research - SA2	4	Research - SA2	5	Research - SA2	2
14.02.23	Research - SA2	4	Research - SA2	4	Research - SA2	4
15.02.23	Research - SA2	5	Research - SA2	5	Research - SA2	5
16.02.23	Research - SA2	4	Research - SA2	4	Research - SA2	4
17.02.23	Meeting with client	1	Meeting with client	1	Meeting with client	1
20.02.23	Research - SA2	4	Research - SA2	4	Research - SA2	4
21.02.23	Physical meeting with client/Research	5	Physical meeting with client/Research	5	Physical meeting with client/Research	5

	Total hours
Petar	497.5
Sindre	496.5
Jo	500.5
Sum	1494.5

22.02.23	Research - SA2	6	Research - SA2	6	Research - SA2	6
23.02.23	Research - SA2	5	Research - SA2	5	Research - SA2	5
24.02.23	Research - SA2 Meeting with client	4	Research - SA2 Meeting with client	4	Research - SA2 Meeting with client	4
27.02.23	Research - SA2	7	Research - SA2	7	Research - SA2	6
28.02.23	Research - SA2	5	Research - SA2	5	Research - SA2	5
01.03.23	Research - SA2	5	Research - SA2	5	Research - SA2	5
02.03.23	Research - SA2	6	Research - SA2	6	Research - SA2	6
03.03.23	Research - SA3 Meeting with client and supervisor	5	Research - SA3 Meeting with client and supervisor	5	Research - SA3 Meeting with client and supervisor	4
06.03.23	Research - SA3	5	Research - SA3	5	Research - SA3	5
07.03.23	Research - SA3	5	Research - SA3	5	Research - SA3	5
08.03.23	Research - SA3	5	Research - SA3	5	Research - SA3	5
09.03.23	Research - SA3	5	Research - SA3	5	Research - SA3	5
10.03.23	Research - SA3 Meeting with client	5	Research - SA3 Meeting with client	5	Research - SA3 Meeting with client	5
13.03.23	Research - SA3	6	Research - SA3	6	Research - SA3	6
14.03.23	Research - SA3	5	Research - SA3	5	Research - SA3	5
15.03.23	Research - SA4	7	Research - SA4	7	Research - SA4	7
16.03.23	Research - SA4	5	Research - SA4	5	Research - SA4	5
17.03.23	Research - SA4 Meeting with client and supervisor	6	Research - SA4 Meeting with client and supervisor	6	Research - SA4 Meeting with client and supervisor	6
20.03.23	Research - SA4, startet working on the report	5	Research - SA4, startet working on the report	5	Research - SA4, startet working on the report	5
21.03.23	Research - SA4	5	Research - SA4	5	Research - SA4	5
22.03.23	Research - SA4	6	Research - SA4	6	Research - SA4	6
23.03.23	Research - SA4	5	Research - SA4	5	Research - SA4	5
24.03.23	Research - SA4 Meeting with supervisor	6	Research - SA4 Meeting with supervisor	6	Research - SA4 Meeting with supervisor	6
27.03.23	Research - SA4	5	Research - SA4	5	Research - SA4	5
28.03.23	Research - SA4	5	Research - SA4	5	Research - SA4	5
29.03.23	Research - SA4	6	Research - SA4	6	Research - SA4	6
30.03.23	Research - SA5	6	Research - SA5	6	Research - SA5	6
31.03.23	Research - SA5 Meeting with client	6	Research - SA5 Meeting with client	6	Research - SA5 Meeting with client	6
11.04.23	Research - SA5	7	Research - SA5	7	Research - SA5	7
12.04.23	Research - SA5	7	Research - SA5	7	Research - SA5	7
13.04.23	Research - SA5	6	Research - SA5	6	Research - SA5	6
14.04.23	Research - SA5 Meeting with client and supervisor	6	Research - SA5 Meeting with client and supervisor	6	Research - SA5 Meeting with client and supervisor	6
17.04.23	Research - SA5	6	Research - SA5	6	Research - SA5	6
18.04.23	Writing report	8	Writing report	8	Writing report	8
19.04.23	Writing report	6	Writing report	6	Writing report	6
20.04.23	Writing report	7	Writing report	7	Writing report	7
21.04.23	Writing report Meeting with client	7	Writing report Meeting with client	7	Writing report Meeting with client	7
24.04.23	Writing report	7	Writing report	7	Writing report	7
25.04.23	Writing report	7	Writing report	7	Writing report	7
26.04.23	Writing report	7	Writing report	7	Writing report	7
27.04.23	Writing report Meeting with supervisor	7	Writing report Meeting with supervisor	7	Writing report Meeting with supervisor	7
28.04.23	Writing report Meeting with client	8	Writing report Meeting with client	8	Writing report Meeting with client	8
01.05.23	Writing report	8	Writing report	8	Writing report	8
02.05.23	Writing report	8	Writing report	8	Writing report	8
03.05.23	Visiting NCSC	8	Visiting NCSC	8	Visiting NCSC	8
04.05.23	Writing report	8	Writing report	8	Writing report	8

05.05.23	Writing report Meeting with client and supirvisor	8	Writing report Meeting with client and supirvisor	8	Writing report Meeting with client and supirvisor	8
06.05.23	Writing report	9	Writing report	9	Writing report	9
07.05.23	Writing report	8	Writing report	8	Writing report	8
08.05.23	Writing report	8	Writing report	8	Writing report	8
09.05.23	Writing and finalize report	8	Writing and finalize report	8	Writing and finalize report	8
10.05.23	Writing and finalize report	8	Writing and finalize report	8	Writing and finalize report	8
11.05.23	Writing and finalize report	12	Writing and finalize report	12	Writing and finalize report	12
12.05.23	Writing and finalize report	8	Writing and finalize report	8	Writing and finalize report	8
13.05.23	Writing and finalize report	9	Writing and finalize report	9	Writing and finalize report	9
14.05.23	Writing and finalize report	9	Writing and finalize report	9	Writing and finalize report	9
15.05.23	Writing and finalize report	8	Writing and finalize report	8	Writing and finalize report	8
16.05.23	Writing and finalize report Meeting with supervisor	8	Writing and finalize report Meeting with supervisor	8	Writing and finalize report Meeting with supervisor	8
17.05.23	Writing and finalize report	10	Writing and finalize report	10	Writing and finalize report	10
18.05.23	Writing and finalize report	14	Writing and finalize report	14	Writing and finalize report	14
19.05.23	Writing and finalize report	5	Writing and finalize report	5	Writing and finalize report	5
20.05.23	Finalize report	6	Finalize report	6	Finalize report	6
21.05.23	Finalize report	6	Finalize report	6	Finalize report	6



NTNU

Norwegian University of
Science and Technology