Master thesis project report

A Dynamic Framework Enhancing Situational Awareness in Cybersecurity SOC-IR

JARL ANDREASSEN
MARTIN EILERAAS

SUPERVISOR
Nadia Saad Noori
Lucia Castro Herrera

University of Agder, 2022
Faculty of Engineering and Science
Department of Engineering and Sciences

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

We would first like to thank our thesis advisors Associate Professor Nadia Saad Noori of the Department of Information and Communication Technology at the Univesity of Agder and PhD Research Fellow Lucia Castro Herrera of the Department of Information Systems at the University of Agder. Our weekly and spontaneous meetings have helped balance our progress towards finally finishing this thesis report. Your persistence and endurance with us is admirable and your efforts are greatly appreciated. Nadia, when we "catch you working" at two at night to answer our emails. Lucia, when you review our work on the Constitution Day. Thank you!

We would also like to thank the anonymous experts who sacrificed their time for us and were involved to provide empirical evidence to support our data collection and for giving us your expert opinions on our conceptual framework. And special thanks to our collaborators who took in our project and made it all feasible.

Finally, we would like to express our profound gratitude to our parents and our significant others for providing us with unfailing support and continuous encouragement throughout our years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Kristiansand,
June 3rd, 2022

Jarl Andreassen
Jarl Andreassen

Martin Eileraas
Martin Eileraas

Abstract

Organizations today face a significant challenge in protecting their valuable IT assets. Cyber criminals unlimited to physical boundaries are able to disrupt and destroy cyber infrastructure, deny organizations access to IT services and steal sensitive data. With the purpose of employing socio-technical systems to detect, analyze and respond to these threats, enterprises organize security operations centres at the heart of their entities. As the environment constantly shifts (i.e., in 2020 the corona virus triggered a digital upheaval creating new attack surfaces; today the Ukrainian war have triggered cyber-conflict) the dependency on these systems increases the need for situational awareness. Essentially, having the capability to gather relevant information from the environment, the means to understand the gathered information, and reflecting that gained understanding for the current environment.

This exploratory study examines how such capabilities are operationalized in leading Managed security service providers (MSSPs) providing cybersecurity operations and incident response, and looks at how situation awareness knowledge is constructed through the organizational levels of the enterprise detection & response. In this context, situational awareness span over different levels in the organization starting from team personnel, ending at top management. Thus, providing situational awareness at the different organizational levels is considered a complex process involving various sources of information, different levels of perspective, and different interpretations which trigger a complex set of decision-making processes.

To explore this, we constructed a theory-informed narrative using a theoretical lens that resulted in the formulation of a conceptual framework. Thus, through interviews with practitioners from across the organizational levels of two leading MSSPs; parallel to inquiring about general aspects surrounding the subject of enterprise response, the conceptual framework was validated. The interview responses were then coded using categorization. The analysis informed the development of the conceptual framework, and so the framework was adjusted to account for the findings. Through interpretation of empirical evidence, the result is a final validated framework which models how cybersecurity operations are operationalized in the enterprise detection & response of leading MSSPs. With emphasis on situation awareness, the framework shows how technology, people and processes either support or engage in the perception, comprehension and projection of situation awareness knowledge in order to make informed decisions. Consequently, the framework takes into account the activities held post-incident to reflect upon the response, which we argue allows for the construction of team situation awareness.

Our work contributes to situation awareness theory in the context of cybersecurity operations and incident response by advancing the understanding of the organizational capabilities of MSSPs to develop awareness of the cyber-threat landscape and the broader operational dynamics. By introducing the dynamic framework enhancing situation awareness in cybersecurity SOC—IR we expand on the models of Endsley (1995) and Ahmad et al. (2021) by combining elements of existing work with empirical findings to reflect best practices applied in MSSPs.

Contents

Acknowledgements **ii**

Abstract **iii**

List of Figures **vi**

List of Tables **vii**

List of Abbreviations **vii**

1 Introduction **1**
1.1 Rationale and motivation 3
1.2 Research approach 3
1.3 Thesis overview 4

2 Background and related work **5**
2.1 Literature Review 5
2.1.1 Method 5
2.1.2 Literature criteria 6
2.1.3 Search process 6
2.1.4 Screening 8
2.2 The role of cybersecurity in organizations 11
2.3 Security Operations Center (SOC) & IR 12
2.3.1 Architecture 12
2.3.2 Roles and responsibilities 12
2.3.3 Processes 13
2.4 Security Information and Event Management (SIEM) 17
2.5 Cyber threat intelligence (CTI) 20
2.5.1 Information exchange 20
2.6 Situational awareness 21
2.6.1 Cybersecurity situation awareness 22
2.7 Theoretical lens 23
2.7.1 Situation awareness of the environment 23
2.7.2 Situation awareness in cybersecurity IR 24
2.7.3 Information flow and communication pathways in IR 27

3 Research approach **29**
3.1 Qualitative approach 29
3.2 Research Design 31
3.3 The unit of analysis and subject selection 32
3.4 Data collection 34
3.4.1 Interview methodology 34
3.5 Limitations of interviews 36

3.6 Data analysis . . . 37
3.7 Ethical considerations . . . 37

4 Results **38**
4.1 The conceptual framework . . . 38
4.2 Empirical findings . . . 40
4.2.1 Data collection of the environment . . . 40
4.2.2 Threat intelligence team . . . 42
4.2.3 The operational level: Handling low-severity incidents . . . 44
4.2.4 Response to high-severity incidents . . . 46
4.2.5 The aftermath . . . 48
4.2.6 Information sharing . . . 50
4.3 Practitioners input . . . 51

5 Discussion / Summary of findings **54**
5.1 A Dynamic Framework of Situational Awareness in Cybersecurity SOC-IR . 55
5.1.1 Operational level . . . 56
5.1.2 Tactical level . . . 57
5.1.3 Strategic level . . . 58
5.1.4 The aftermath . . . 61

6 Conclusion **63**
6.1 Contribution to theory and industry . . . 65
6.2 Limitations and opportunities for further research . . . 65

A Interview Questions **67**

B Interview Guide **69**

C Consent Form **71**

Bibliography **79**

List of Figures

1.1 Process map 4

2.1 Process of systematic literature review (Xiao and Watson, 2019) 6
2.2 Preliminary systematic literature review 8
2.3 Final systematic literature review 9
2.4 Incident Response Life Cycle (Cichonski et al., 2012) 14
2.5 The data collection process. (Vielberth et al., 2020) 14
2.6 Detection & Analysis (Cichonski et al., 2012) 15
2.7 Containment, Eradication & Recovery (Cichonski et al., 2012) 16
2.8 Post-Incident Activity (Cichonski et al., 2012) 17
2.9 A typical SIEM system architecture (Bhatt et al., 2014) 18
2.10 Situation Awareness (Adapted from Endsley) (Ahmad et al., 2021) 24
2.11 Situation Awareness in Cybersecurity IR (Ahmad et al., 2021) 25
2.12 Levels of SA (grounded in theory of (Ahmad et al., 2021)) 26
2.13 Information flow and communication pathways in IR (Ahmad et al., 2021) . 27

3.1 A Map of Genres in Qualitative Research (Sarker et al., 2018) (redacted) . . 32
3.2 A framework for the development of a qualitative semi-structured interview guide (Kallio et al.) 35

4.1 A conceptual framework of SA in SOC IR 39
4.2 Threat-Based Situational Awareness Updates decision tree 45
4.3 Event log (recreation) 49
4.4 Lessons learned (recreation) 50

5.1 A Dynamic Framework Highlighting Situation Awareness in Cyber IR 55
5.2 Operational level dynamics 56
5.3 Tactical level dynamics 57
5.4 SOC-IR dynamics 58
5.5 Strategic level dynamics 59
5.6 'Situation Awareness' process model (Endsley, 1995) 60
5.7 Decision & Action Execution 61
5.8 The aftermath 62

List of Tables

2.1 Keywords used in the search string 7
2.2 Reviewed articles 11
2.3 Advantages and disadvantages with SIEM 19

3.1 Qualitative VS Quantitative aspects (Hennink et al., 2020) 30
3.2 Organizational profile of the two investigated organizations 33
3.3 Subject selection 34

List of Abbreviations	
SA	Situational awareness
MSSP	Managed security service providers
SME	Small and medium-sized enterprise
LSE	Large scale enterprise
IT	Information technology
IS	Information system
APT	Advanced Persistant Threat
PC	Personal computer
DBIR	Data breach investigations report
SOC	Security Operation Center
SLT	Security Leadership Team
IR	Incident response
IRT	Incident Response Team
SA-CIR	Situation Awareness in Cybersecurity Incident Response
CISO	Chief Information Security Officer
CIO	Chief Information Officer
EM	Emergency manager
ICS	Industrial Control System
SLR	Systematic Literature Review
CTI	Cyber threat intelligence
CSIRT	Computer Security Incident Responce Team
CERT	Computer Emergency Response Team
SOP	Standard Operating Procedures
CSMS	Cyber Security Management System
ITSM	IT Service Management
SIEM	Security Information and Event Management
MI	Major Incident
MIT	Major Incident Team
IOC	Indicator of Compromise
NIST	National Institute of Standards and Technology
DDoS	Distributed denial-of-service attack
IDPS	Intrusion Detection and Prevention System
KPI	Key Perfomance Indicator
RQ	Research question
HTTP	Hypertext Transfer Protocol
URL	Uniform Resource Locator
GPO	Group Policy Object
TLP	Traffic Light Protocol
TTP	Tactics, Techniques and Procedures
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
CIS	Cybersecurity Information Sharing
ECA	European Economic Area
ENISA	The European Union Agency for Cybersecurity
EU	European Union
SSI	Semi-structured interviews
NSD	Norwegian Centre for Research Data
L1, L2, L3	Level 1,2,3
C-suite	Executive-level manager within a company

Chapter 1

Introduction

Cybersecurity threat actors have risen to become increasingly sophisticated, persistent and organized, posing a substantial threat to modern organizations (Ahmad et al., 2021). Verizon's 2021 data breach investigations report (DBIR) reported that external threat actors in 2020 perpetrated 80 percent of recorded data breaches, with likewise 80 percent of *top threat actor varieties* in breaches committed by organized crime groups (Verizon, 2022). Human attackers who are well-informed, well-trained and methodical by *modus operandi* use sophisticated tools and techniques to disrupt and destroy critical cyber infrastructures, deny organizations access to their own IT infrastructures and services, and steal sensitive data such as intellectual property, trade secrets, and customer data. As a result, organizations may suffer from a loss of competitive advantage, productivity, reputation, and customer confidence, as well as legal penalties and direct financial loss (Ahmad et al., 2021).

The 19th of March 2019 the Norwegian aluminium-giant Hydro was struck by an extensive ransomware attack known as Lockergoga. Screens at factories and plants around the world went black, and the company had to switch to manual processes in a number of countries, while PCs had to be turned off and all communication had to take place on improvised platforms. The company refused to pay the hackers' (an Advanced Persistent Threat (APT) group known as FIN6) bitcoin ransom demands, and issued a stock exchange announcement a few hours after the attack was discovered. The attack affected the whole of their global organisation and led to extensive operational challenges including large economic losses. To recover from the attack, all PCs and servers throughout the organisation were crawled, cleaned of malicious software and then restored to ensure security. Entire systems; encrypted PCs and servers had to be rebuilt based on security backups. Hydro subsequently had to re-organize their entire security team to better be able to detect and respond to such an attack again. Today, they estimate the total cost of the cyber attack to be upwards of 75 million dollars (Hydro, 2020; Klevstrand et al., 2020). Despite having a dedicated security team and what was thought to be sufficient security measures in place to defend the organization, the attack on Hydro is a prominent example of the very real threat that looms in cyberspace today and how vulnerable organizations are in the current environment.

The growing dependency on cyberspace has greatly increased the need for situational awareness —essentially, perceiving and understanding the operational environment and accurately predicting and responding to problems that might occur (Mitre.org, 2022). Situational awareness is the process of getting relevant information from across the organization, integrating it into usable intelligence, and re-disseminating it out to help people throughout the organization to make better decisions (Horneman, 2019). The systems and networks that operate in cyberspace have vulnerabilities that present significant risks to both individual organizations and national security. By anticipating what might happen to these systems, leaders can develop effective countermeasures to protect their critical missions. Hence, situational awareness span over different levels in the organization starting from the cybersecurity team personnel, ending at the top management level. Thus, providing situational awareness at the different organizational levels is considered a complex process involving various sources of information, different levels of perspective, and different interpretations which trigger a complex set of decision making processes (Mitre.org, 2022).

A press release from the world's leading information technology research and advisory company (Gartner, 2021) stated that worldwide spending on *information security and risk management technology and services* were forecast to grow 12.4 percent to reach 150 billion dollars in 2021, as it grew 6.4 percent in 2020. Furthermore, their CIO Agenda Survey (Gartner, 2020) found that cybersecurity was the top priority for new spending, with 61 percent of the more than 2,000 CIOs surveyed reported increasing investment in cyber/information security that year. A Deloitte (2019) survey of 500 C-level executives further reports that more than 15 percent of organizations outsource security operations to security service providers, while 99 percent outsourced some portion of their cybersecurity operations in total. In an article about situation awareness, Mitre.org (2022) have highlighted the status of situational awareness in organizations —enlightening that situational awareness on the technology level is 'available today', whilst situational awareness catering to the needs of the operational and strategic levels are either evolving or lacking. This is supported in existing literature. For example, one study (Oyewole, 2016) reveals that a majority of cybersecurity incidents are caused by employees lacking situational awareness, stating that organizations build detection and incident response capabilities based on the available technology components without paying sufficient attention to the people or process dimensions of the solutions. Another study (Ahmad et al., 2021) reveals that most research on the subject of situational awareness has focused on the technological perspective with comparatively less focus on the practice perspective, and suggests that situational awareness is a critical attribute of incident detection and response.

As the field of incident response advances technologically, it is imperative that human factors efforts keep pace in representing the human half of the human-machine system (Nyre-Yu et al., 2019). We therefore pose the following research questions addressing the practical perspective of situational awareness:

- "How are leading Managed security service providers (MSSPs) operationalized to provide security operations and incident response as a service?"

- "How is situational awareness knowledge constructed through the organizational levels of the MSSP?".

The purpose of this exploratory study is to develop an understanding of the concept of situation awareness and its relation to cybersecurity; investigate its function in the context of enterprise MSSP security operations and examine how situation awareness knowledge is constructed through the organizational levels of the enterprise response. With this knowledge, the objective of the study is to develop and validate a conceptual dynamic framework visualizing the workings of best practice security operations teams.

1.1 Rationale and motivation

A review of literature by Ahmad et al. (2021) suggests that Situation Awareness is a critical attribute of organizational incident response. In their studies, they found that there had been invested considerable effort in studying the technological aspects of developing Situation Awareness but comparatively there had been considerably less focus on the practice perspective. Mitre.org (2022) and Oyewole (2016) states that the society today has access to the technological solutions catering to the needs of situational awareness, yet we are lacking maturity on the operational and strategic levels catering to the needs of threat context and mission [situation] awareness. Evesti et al. (2017) states that the general research community indeed has approached the topic from various perspectives, but reveals that research in the area has focused mostly on industrial control systems (ICS) and system availability. From another perspective, Jajodia and Albanese (2017) states that the current state-of-the-art in the area of automation sees the operational aspects of IT security too time-consuming to allow for the focus on the process perspective of situation awareness in most realistic scenarios. On the other hand, as a motivation to pursue this angle, Rajivan and Cooke (2017) mentions in their recommendations for further research that 'it would be beneficial to use study opportunities for studying work flow of cyber defense analysts and cognitive processes underpinning their work flow'. In "response" to their suggestion for further research, our study focuses on the cognitive processes of situation awareness in security analysts and major incident teams visualizing the communication pathways and information flows between them including the broad operational context.

1.2 Research approach

To examine and understand the concept of enterprise detection and response and what comprises situational awareness within a large scale MSSP context, this study uses a qualitative research approach. The technique for data gathering in this research is primarily through semi-structured interviews and research articles from reputable journals. The study began with a preliminary systematic literature review of eleven articles, that took place between September and November of 2021. With the goal of developing an understanding of the concept and phenomenon of situation awareness in cybersecurity, this established a foundation of knowledge for the primary literature review of twenty-one articles which took place between January and February of 2022. For the interviews we chose a qualitative approach as they are aimed to extract comprehensive information, making them particularly valuable when studying social processes and the "how" of various occurrences. Twelve interviews were thus carried out between March and April of 2022, which lasted between fifty to seventy minutes each, with respondents from two leading MSSPs based in Norway. The first set of questions established the interviewee's role and responsibilities as well as their take on what situation awareness in cybersecurity means to them and their company. The second set asked the interviewee to walk the researchers through the different technologies, standards and frameworks used within incident management and how they cooperate with other organizations to enhance situation awareness. The third and fourth set of questions dealt with the company's incident response process to major cybersecurity incidents and what the respondent saw as the biggest challenges associated with such an incident. In the last part of the interview we presented and explained our proposed conceptual framework with follow-up questions, with the point of validating whether our theory-informed framework represents how MSSP security operations works in real life. The systematic literature review and the semi-structured interviews respectively provided the theoretical foundation and empirical findings so that it was possible to answer the research questions. In figure 1.1, we present a "process map" that models our research approach and the processes reviewed to reach a conclusion.

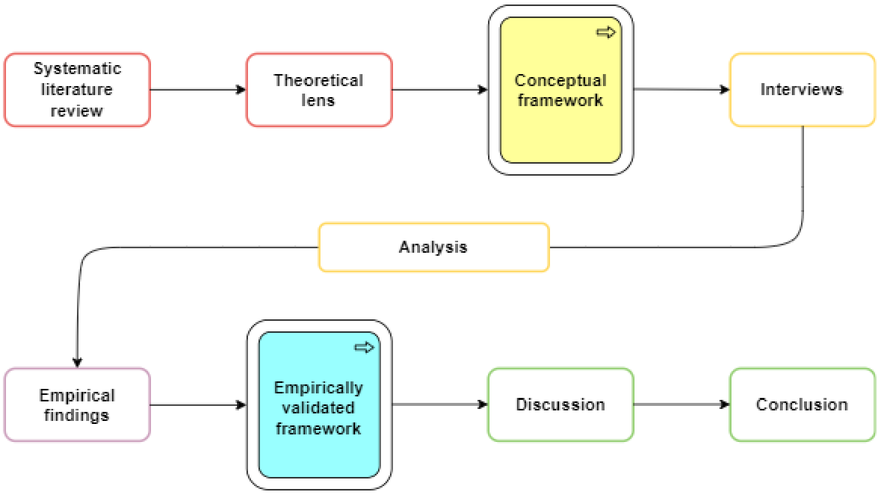


Figure 1.1: Process map

1.3 Thesis overview

Chapter 1 - Introduction provides an overview of the problem statement and the research questions.

Chapter 2 - Background and related work discusses the literature review process as well as the background and related research that form the foundation of this study. Introduces the theoretical lens from which our conceptual framework is informed.

Chapter 3 - Research approach presents arguments for why the chosen research approach and its philosophical assumptions is suitable for this study. Moreover, research design, data collection, interview methodology, limitations of interview, data analysis, validity and ethical considerations are presented.

Chapter 4 - Results is where we present the conceptual framework and address the findings collected from the interviews.

Chapter 5 - Discussion is where we present the empirically validated framework and the literature is discussed with the empirical findings.

Chapter 6 - Conclusion Provides a conclusion and a brief reflection of limitations and opportunities for further research as well as the contribution to theory and industry.

Chapter 2

Background and related work

In this section we discuss the literature review process, including the choice of method, literature criteria, search and screening process before presenting an overview of the articles reviewed. Subsequently, we discuss the background and related research that form the theory of this study before introducing the theoretical lens from which our coming conceptual framework is informed.

2.1 Literature Review

The systematic literature review (SLR) provides an analytical review of literature that is relevant for the thesis project. The primary motivation for conducting an SLR was to provide greater insight and understanding of the phenomenon 'situational awareness' in cybersecurity and how it is operationalized in enterprise detection and response. Aligned with Kitchenham and Charters (2007), our rationale for choosing the SLR approach is that it is a well-defined methodology making it less likely that the results are biased and that they can provide information about the effects of a phenomenon across a wide range of settings and empirical methods, providing evidence that a phenomenon is robust and transferable. The major weakness though is that it requires considerably more time and effort than traditional literature reviews.

> *"To push the knowledge frontier, we must know where the frontier is. By reviewing relevant literature, we understand the breadth and depth of the existing body of work and identify gaps to explore."* (Paré et al., 2015)

2.1.1 Method

Before starting our research, we did a preliminary SLR to establish a theoretical foundation. Then we ran a new "screening" on the previous SLR and took with us only the articles that we considered were relevant to our coming research after gaining a greater understanding of the subject. Then we completed a fresh "screening" before "snowballing" from these articles, shaping the new literature review. We chose to follow a SLR approach to select and identify research to help reach our objectives, accommodating the research questions. A systematic literature review is a means of identifying, evaluating and interpreting research relevant to a particular research question, or topic area, or phenomenon of interest (Kitchenham and Charters, 2007).

Based on the framework of Kitchenham (2004), the model below (figure 2.1) of Xiao and Watson (2019) represents our process steps. The reason for this choice is, as it is written about "the most common reasons for choosing SLR" in Kitchenham and Charters (2007)' framework guide; *"To provide a framework/background in order to appropriately position new research activities"*. This relates to our subsequent qualitative study where we construct a theory-informed narrative using a theoretical lens that through empirical inquiry results in the formulation of a conceptual framework. *"Ideally, a systematic review should be conducted before empirical research, and a subset of the literature from the systematic review that is closely related to the empirical work can be used as background review."* (Xiao and Watson, 2019)

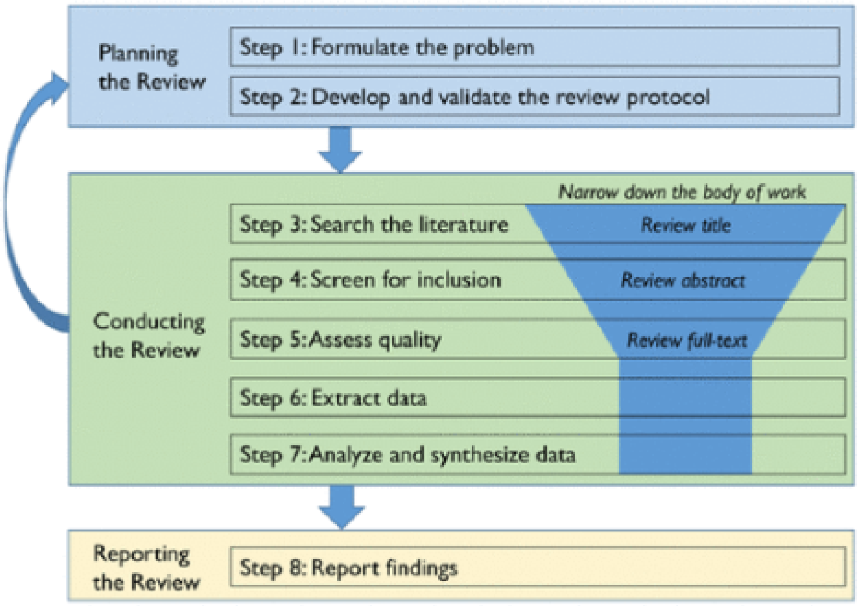

Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Conducting the Review
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 2.1: Process of systematic literature review (Xiao and Watson, 2019)

2.1.2 Literature criteria

Criteria need to be set regarding the related research to help us accumulate results that correlates to the research problem to a higher degree.

- The articles must be written in English or Norwegian
- The articles must contain a combination of keywords relating to our research problem
- The articles should be published in a trustworthy journal
- The articles should have been peer-reviewed
- The articles should not be older than 7 years. However, if the content of the paper is relevant for today, it could be included regardless of the publication date.
- Literature cited by more sources will be prioritized over similar articles with fewer citations

2.1.3 Search process

The literature search process finds material for the review; hence, a systematic review depends on a systematic search of literature. When looking for relevant literature, the three major sources that are considered are; (1) electronic databases, (2) backward searching and (3) forward searching. Electronic databases constitute the predominant source of published literature collections (Patticrew and Roberts, 2006). During the literature review process, we used the search engines and databases IEEE Xplore, Scopus, and Google Scholar to find relevant literature. These search engines provides adequate results, as they collect literature from multiple sources and provide a comprehensive library of content. Relevant literature was retrieved and stored utilizing cloud storage software during the search. In order to find relevant literature, we made a set of key-words that were used in formulating the search strings (see table 2.1). Our approach was to make one broader search with more keywords and more liberal operators (i.e. Situation awareness OR Security readiness) and one narrower search with more strict use of operators (i.e. "Situation Awareness" AND "Incident response").

Keyword	**Synonym/related concept (Abbreviation)**
Cybersecurity	- *Cyber Security* - *Cyber Defence* - *IT Security* - *Computer Security* - *Information Security*
Situational Awareness	- *Situation Awareness (SA)* - *Security Readiness* - *Security Awareness*
Incident Management	- *Cyber Security Management* - *Information Management* - *Incident Response (IR)* - *IR Life Cycle*
Cyber Threat Intelligence	- *Threat Intelligence* - *(CTI)*
Security Operation Center	- *(SOC)* - *Computer Security Incident Responce Team (CSIRT)*
Security Information and Event Management	- *(SIEM)*
Information Sharing	- *Information Exchange* - *Information Dissemination* - *Threat Intelligence Sharing* - *Knowledge Sharing*
Enterprise/organization	- *Organisation* - *Firm* - *Company* - *Managed Security Service Provider (MSSP)*

Table 2.1: Keywords used in the search string

2.1.4 Screening

After compiling a list of references, researchers should further screen each article to decide whether it should be included for data extraction and analysis (Xiao and Watson, 2019). According to the selection protocol and the article criteria established, after compiling a reference list from the initial and supplementary searches, we conducted a screening process to include and exclude literature. To visualize the process, a PRISMA flow diagram is presented in figure (2.2) below.

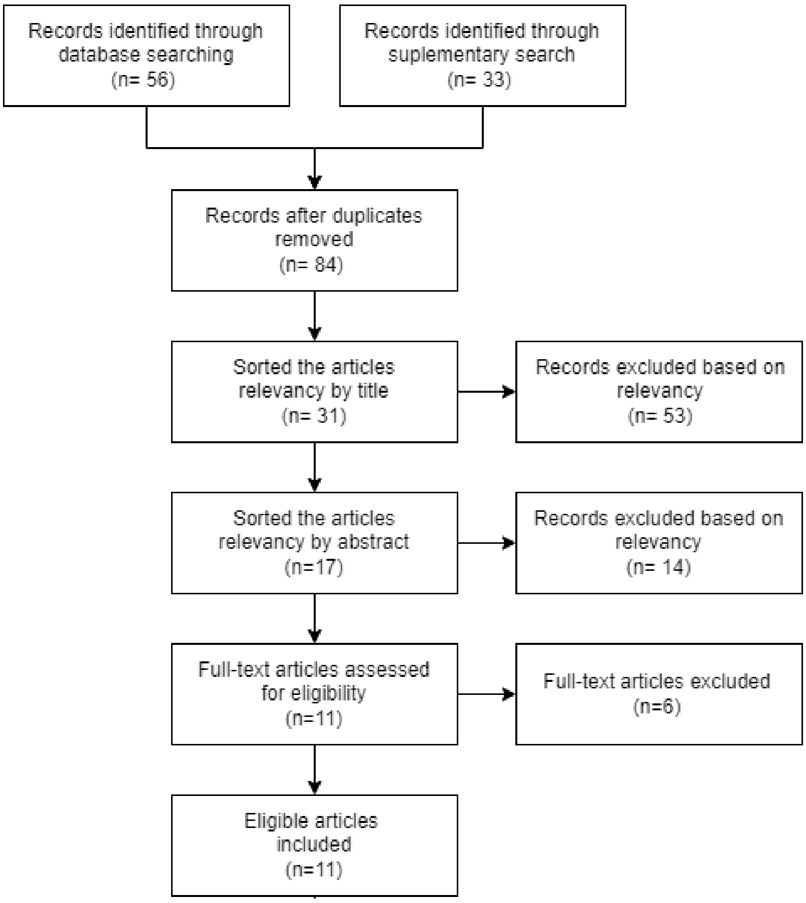

Records identified through database searching (n= 56)
Records identified through suplementary search (n= 33)
Records after duplicates removed (n= 84)
Sorted the articles relevancy by title (n= 31)
Records excluded based on relevancy (n= 53)
Sorted the articles relevancy by abstract (n=17)
Records excluded based on relevancy (n= 14)
Full-text articles assessed for eligibility (n=11)
Full-text articles excluded (n=6)
Eligible articles included (n=11)

Figure 2.2: Preliminary systematic literature review

The process started by accumulating a list of references from the two searches. After removing duplicates, 84 articles remained. Articles with titles of utter irrelevancy were excluded, i.e. titles of which did not represent any relevance to the study. Thereafter, by the remaining 31 articles, abstracts were read to conclude whether they were relevant, similarly to the title screening. After abstract screening we were left with 17 articles. These were then assessed by full-text screening, i.e. reading the most representative information of each article by summaries, findings, results, conclusions and selected chapters for relevancy while simultaneously assessing the quality of the works, which excluded 6. The screening process left us with 11 articles.

Following the preliminary research to gain a basic understanding of the topic, we realized that we needed to reconsider some of the articles, and supplement with an additional search process. As our knowledge of the relevant concepts improved, the scope of the project shifted. Thus, we realized that some articles were no longer relevant to the study. Furthermore we developed a basis to conduct more relevant and accurate searches. To obtain the necessary and relevant literature that would form the theory and background of this study we conducted an additional search. Following the same principles as with the preliminary SLR, we concluded the process with a snowballing approach from the 13 eligible articles identified. The PRISMA flow diagram below (see figure 2.3) depicts the results of the final screening process.

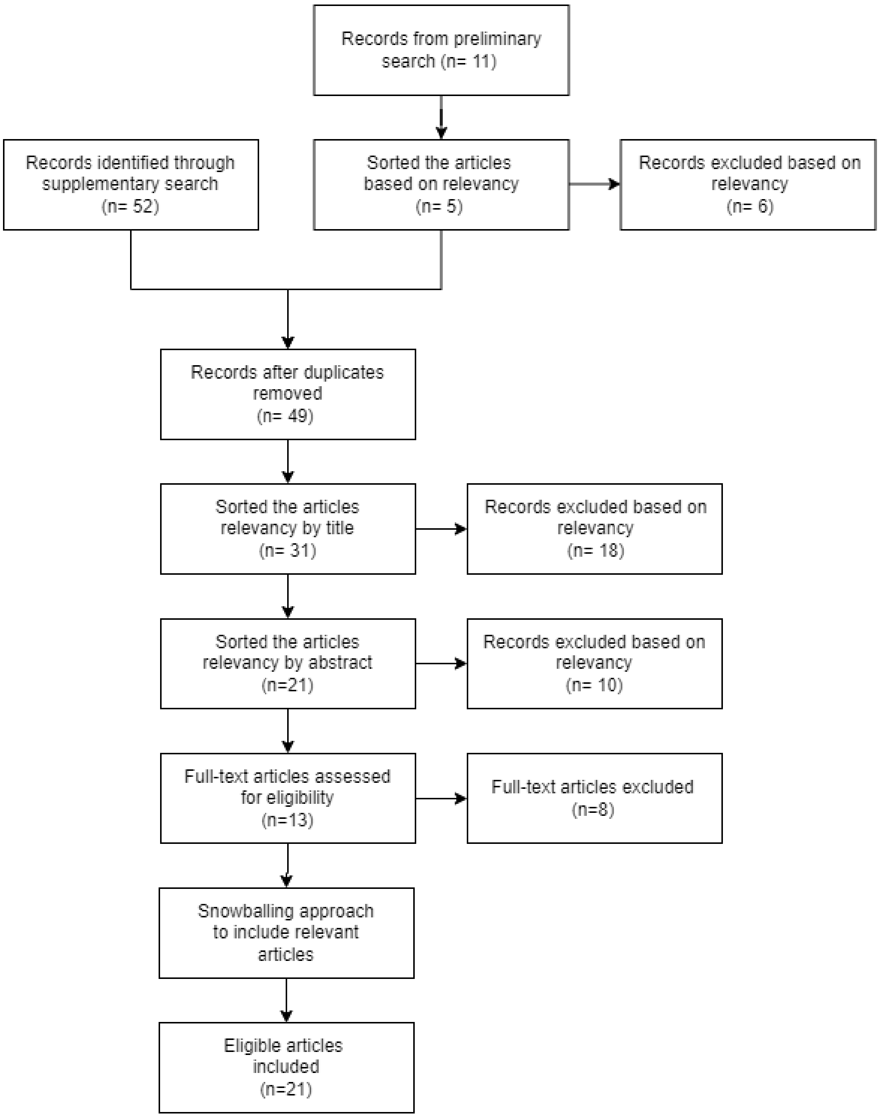

Records from preliminary search (n= 11)
Records identified through supplementary search (n= 52)
Sorted the articles based on relevancy (n= 5)
Records excluded based on relevancy (n= 6)
Records after duplicates removed (n= 49)
Sorted the articles relevancy by title (n= 31)
Records excluded based on relevancy (n= 18)
Sorted the articles relevancy by abstract (n=21)
Records excluded based on relevancy (n= 10)
Full-text articles assessed for eligibility (n=13)
Full-text articles excluded (n=8)
Snowballing approach to include relevant articles
Eligible articles included (n=21)

Figure 2.3: Final systematic literature review

The 21 eligible and selected articles from the screening process are presented in the table (2.2) below.

Author (Year)	**Source**	**Title**	**Keywords**
Conti, et al., (2018)	Advances in Information Security	Cyber Threat Intelligence: Challenges And Opportunities	Cyber Threat Intelligence, Indicators of attack Indicators of compromise, Artificial Intelligence (AI)
Hasan, et al., (2021)	Information security and Applications	Evaluating the cyber securityreadiness of organizations and its influence on performance	Cyber security, Readiness, TOE framework, Security performance, Financial performance, Non-financial performance
Karen Kent, Murugiah Souppaya, (2006)	NIST	Guide to Computer Security Log Management	Security software, Log protection, Log analysis Syslog format, Syslog security, Architecture

Author (Year)	Source	Title	Keywords
Ahmad, et al., (2021)	Computers & Security	How can organizations develop situation awareness for incident response: A case study of management practice	Cybersecurity management, Information security management, Incident response, Cybersecurity, Situation awareness, Case study,
Wagner, et al., (2019)	Computers & Security	Cyber threat intelligence sharing: Survey and research directions	Advanced persistent threat, Cyber threat intelligence, Threat sharing, Relevance, Trust, Anonymity, Literature survey
Evesti, A.; Kanstrén, T.; Frantti, T., (2017)	IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)	Cybersecurity situational awareness taxonomy	Computer security, Taxonomy, Decision making, Monitoring, Law, Decision making, security of data
Jajodia, S.; Albanese, M., (2017)	Center for Secure Information Systems, George Mason University	An Integrated Framework for Cyber Situation Awareness (Part of book: Theory and Models for Cyber Situation Awareness)	Framework, Cyber Situation Awareness
Franke, U,; Brynielsson, J., (2014)	Computers and Security	Cyber Situational Awareness - A systematic review of the literature	Situational awareness, Cyber security, National cyber strategies, Research strategy, Literature review
Scott E. Jasper (2016)	International Journal of Intelligence and Counter Intelligence	U.S. Threat Intelligence Sharing Frameworks	Cyber threat intelligence configurations, Sharing coordination challenges, Automated mechanisms
Oyewole, T., (2016)	ISACA Journal	Application of Situation Awareness in Incident Response	Perception, Comprehension, Projection, Situation awareness theory, IR detection, Analysis, Improvement
K. Oosthoek,. C. Doerr, (2021)	International Journal of Intelligence and Counter Intelligence	Cyber Threat Intelligence: A Product Without a Process?	CTI, Cyber threats, IoC, APT, Artificial intelligence (AI)
J. M. de Fuentes et al. (2017)	Computers & Security	PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing	Cybersecurity information sharing, Cyberthreat management, Format preserving encryption, Homomorphic encryption, Cooperative cyberdefense
R. van der Kleij, et al., (2022)	Computers & Security	Developing decision support for cybersecurity threat and incident managers	Cybersecurity, Cognitive task analysis, Cognitive work analysis, Decision support, Incident response, Information security risk management
C. Goodwin et al. (2015)	Microsoft Security	A framework for cybersecurity information sharing and risk reduction	Situational awareness, Framework, Mitigations, Best practices, Microsoft security

Author (Year)	Source	Title	Keywords
P. Rajivan & N. Cooke., (2017)	Theory and models for Cyber Situation Awareness (Computer Science book series)	Impact of Team Collaboration on Cybersecurity Situational Awareness	Teamwork, Collaboration, Communication, Human factors, Cyber security, Simulation, Modeling, Cognitive Task Analysis, EAST
M. Nyre-Yu, et al., (2019).	Sage Journals	Observing Cyber Security Incident Response: Qualitative Themes From Field Research	Incident response, CSIRTs, Information sharing, Organization, Learning, Automation
S. Barnum (2014).	The MITRE Corporation	Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression	STIX, CTI, Information sharing, Standardization
S. Bhatt, et al., (2014).	IEEE Security & Privacy	The operational role of security information and event management systems	Security information and event management systems (SIEM), Security operation center SOC, Network security
K. Arlitsch, A. Edelman (2014).	Journal of Library Administration	Staying Safe: Cyber Security for People and Organizations	Responsibility, Integrity, Confidentiality, Availability
M. Vielberth, et al. (2020)	IEEE Access	Security Operations Center: A Systematic Study and Open Challenges	SOC, Security of data, Computer security, Security management, Cyber incidents
O. Podzins, A. Romanovs	IEEE Conference of Electrical, Electronic and Information Sciences	Why SIEM is Irreplaceable in a Secure IT Environment?	SOC, SIEM, IT infrastructure, Computer security, Log analysis, Incident management

Table 2.2: Reviewed articles

2.2 The role of cybersecurity in organizations

As Hasan et al. (2021) defines cybersecurity, it is the practice of protecting an organization's IT-related assets, including data, systems and networks, from digital attacks that may access, destroy, or change sensitive information or disturb business operations. Cybersecurity involves the convergence of people, processes and technology to protect organizations, individuals or networks from digital attacks. Organizations that manage and preserve sensitive data must take their obligations seriously and allocate adequate resources to ensure the data's protection, and organizational leadership must encourage a culture of responsible data management and demand that cyber security be taken seriously (Arlitsch and Edelman, 2014).

Ursillo and Arnold (2019) explains that the purpose of any cybersecurity strategy is to assure data confidentiality, integrity, and availability. Confidentiality refers to how information is organized in terms of who needs access and how sensitive the information is. The certainty that the data has not been tampered with or deteriorated during or after submission is referred to as data integrity. Data availability denotes the availability of information to authorized users when it is required (DNV, 2022). New threats develop on a regular basis, and each organization must ensure that it is prepared to deal with a constantly changing threat landscape, and even though organizations have significantly increased their investments in cybersecurity in later years, incident occurrences have continued to rise (Ahmad et al., 2021).

In order to detect intrusions efficiently, a global view of the monitored network is required. This is only possible with an architecture that can collect data from all sources. This task is specifically assigned to a Security Operation Center (SOC) (Bidou et al., 2004).

2.3 Security Operations Center (SOC) & IR

We ground theory about SOCs on a systematic study. The study by Vielberth et al. (2020) reviewed 158 academic publications to determine the current state-of-the-art knowledge within SOCs of which it derived the primary building blocks that it comprises. Using this knowledge we develop an understanding of the general aspects of SOC relevant to our study.

2.3.1 Architecture

A SOC is an organizational entity that is at the heart of all security operations. It is usually viewed as a complex structure that manages and improves an organization's total security posture rather than a single entity or system. Its job is to employ technology, people and processes to detect, analyze, and respond to cybersecurity threats and incidents (Vielberth et al., 2020).

On a high and abstract level, SOCs can be structured as centralized, distributed, or decentralized entities. A centralized architecture in the context of SOCs refers to the approach in which all data is transferred from various locations or subsidiaries to a single central SOC for processing. A distributed SOC resembles one single system operating across several subsidiary companies. Users have the impression that they are interacting with one single entity. All entities can retrieve, process, integrate, and deliver security information and services to other entities using the distributed system. A decentralized SOC is made up of a few SOCs of possibly limited capability that report to one or more central SOCs (Vielberth et al., 2020). Adding to that, Muniz et al. (2015) state that the choice of architecture should formalize the operation model of SOC in terms of components and relationships.

2.3.2 Roles and responsibilities

Depending on the scope and size of the SOC, different teams are needed in different numbers. Different tiers of analysts, as well as dedicated managers, are typical core positions within the operational hierarchy:

- **Tier 1** analysts are primarily in charge of gathering raw data and assessing alarms and alerts from system monitoring tools. They confirm, determine, or revise the criticality of alerts, as well as add important data to them. The analyst determines if each alarm is legitimate or a false positive (Vielberth et al., 2020). If the analyst receives too many false alarms, the rule that specify alarm criteria is escalated for reconfiguration to a SOC engineer (Bhatt et al., 2014). Identification of other high-risk events and possible incidents is another job at this level. All of these must be prioritized based on their importance. If problems can't be resolved at this level, they're escalated to tier 2 analysts (Vielberth et al., 2020).

- **Tier 2** analysts evaluate the more serious security incidents escalated by tier 1 analysts and conduct a more in-depth analysis using threat intelligence (Indicators of Compromise (IOC), updated rules, etc.). They must comprehend the scale of an incident and be aware of the systems that are affected on a higher level. At this tier they transform the raw attack telemetry data collected at tier 1 into actionable threat intelligence (Vielberth et al., 2020). Tier 2 security analysts use a broader range of information to conduct deeper analysis, including internal sources such as system logs and asset management systems, as well as external sources such as threat activity alerts from government agencies and private corporations (Bhatt et al., 2014). Furthermore, designing and implementing measures to contain and recover from an incident is the responsibility of tier 2 analysts. If a tier 2 analyst face major issues with identifying or mitigating a cyberattack, additional tier 2 analysts are consulted, or the incident is escalated to tier 3 (Vielberth et al., 2020).

- **Tier 3** analysts are the most experienced members of a SOC's workforce. They deal with major incidents that have been escalated to them by tier 2 analysts. Analysts at this level also conduct or supervise vulnerability assessments and penetration testing in order to identify attack vectors. Their primary role is to identify potential threats, security flaws, and vulnerabilities before they become known. Moreover, they should recommend ways to optimize the deployed security monitoring tools as they gather reasonable knowledge about a potential threat to the systems. At this level, analysts must also analyze all significant security alerts, threat intelligence, and other security data provided by tier 1 and tier 2 analysts (Vielberth et al., 2020).
- **SOC Managers** oversee the security operations team. They provide technical assistance as needed, but most importantly, they are responsible for effectively managing the team. Evaluating team members, developing processes, assessing incident reports, and developing and implementing necessary crisis communication plans are all part of the job. They also assist with security audits, and report to the Chief Information Security Officer (CISO) or other top-level management position (Vielberth et al., 2020). Managers are ultimately responsible in making sure that incident response activities are carried out correctly(Cichonski et al., 2012).

These core roles are present in all SOCs, regardless of size. However, in a smaller SOC, each role's responsibilities are broader, and as the SOC grows, they are narrowed down to be more specific. In a small SOC with only a few analysts, for example, everyone must be knowledgeable in several skills because a few employees must cover all arising tasks. Roles in a larger SOC can be more specific, such as some analysts focusing on network monitoring while others are experts in e.g., cloud or on-premises specifics (Vielberth et al., 2020). Muniz et al. (2015) also notes that SOC responsibilities could be outsourced to a managed service provider.

On another side-note, the terms CSIRT (Computer Security Incident Response Team) and SOC are frequently interchanged, despite the fact that CSIRTs focuses primarily on the response phase after an incident has occurred. A CSIRT is an organizational entity in charge of coordinating and assisting the response to a cyber incident. A CSIRT can be characterized as a stand-alone unit or as part of a SOC (Vielberth et al., 2020). At the tier 3, Muniz et al. (2015) states that a CSIRT is often involved to deal with an incident, brought in by tier 3 analysts.

2.3.3 Processes

Because the goal of a SOC is to respond to and prepare for incidents, one approach to structuring the underlying processes is to use the Incident Response Lifecycle or similar frameworks such as the ISO/IEC 27035:2016. The Incident Response Lifecycle, according to the NIST Computer Security Incident Handling Guide, consists of four steps: "preparation," "detection and analysis," "containment, eradication, and recovery," and "post-incident activity," which will form the structure of the following section (Vielberth et al., 2020) (see Figure 2.4).

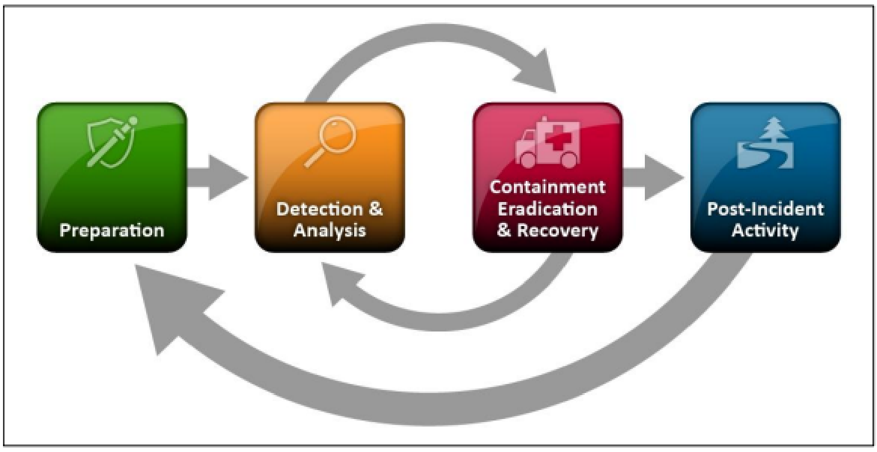


Figure 2.4: Incident Response Life Cycle (Cichonski et al., 2012)

Preparation

The preparation step of the incident response cycle within SOC-literature mainly focuses on data collection, according to Vielberth et al. (2020). The identified five process steps of data collection are Normalization, Filtering, Reduction, Aggregation and Prioritization, as can be seen in Figure 2.5 below.

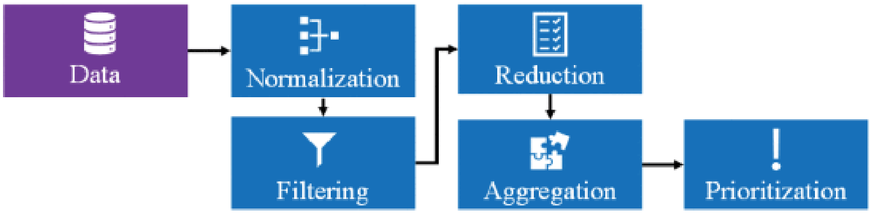


Figure 2.5: The data collection process. (Vielberth et al., 2020)

The following presented sequence is the *most common and uniform* among existing literature and represents *the core steps*, meanwhile there are various data collection processes that can be adopted to enhance the effect of preparation.

1) Normalization is about translating heterogeneous data formats into a standard format to further conduct processing. Normalizing data into uniform representation helps avoid confusion in the timeline of security events and reduces the possibility of incorrect conclusions being drawn based on inconsistently measured network activity. This process is often referred to as pre-processing or log parsing (Vielberth et al., 2020).

2) Filtering is about screening system data for elements that are likely to contain *critical information* from a security standpoint (Vielberth et al., 2020); such as *Robust Filtering* handling syslog (system log) messages differently based on the host or program that generate a message (Kent and Souppaya, 2006).

3) Reduction is about *sorting out* data in logs to reduce redundancy. It is similar to filtering, but works in such a way that it removes individual unimportant data fields as opposed to filtering where you "hold on to" the important data (Vielberth et al., 2020). Through log reduction, as you remove unneeded entries, a new log is created that is smaller and more manageable (Kent and Souppaya, 2006).

4) Aggregation combines similar events into one single data element. Basically, it also reduces redundancy of data by accumulating correlating log entries into one single log message,

which states the type and number of entries aggregated (Vielberth et al., 2020). I.e., in our understanding, "message 1", "message 2", "message 3" is combined to resemble: "message (3)". For example, if a thousand entries that each record a portion of a scan is aggregated, they would be pooled into a single entry that denotes how many hosts were scanned (Kent and Souppaya, 2006).

5) After defining requirements and goals for the log management process, an organization should prioritize those requirements and goals based on the organization's perceived risk reduction and the expected time and resources required to perform log management functions(Kent and Souppaya, 2006). Prioritization is about classifying log data according to importance to facilitate further processing. Prioritizing incoming data, for example, can help you decide how to respond to events or how long to keep logs (Vielberth et al., 2020). Prioritization may also include the use of correlation to provide context for log entries in order for them to be validated (Kent and Souppaya, 2006).

Detection and Analysis

Even for experienced security professionals, the sheer volume of data collected in previous steps can be daunting. Although the number of alerts generated is heavily dependent on the network environment, for manageability, SOCs typically aim for 1,000 to 3,000 alerts per day per tier 1 analyst(Bhatt et al., 2014). *Data analysis* is used to convert this data into useful information, and is essentially a way to make sense of what is collected. Detection methods are used to recognize incidents within the volume of data with the help of automated procedures and human operators (Vielberth et al., 2020).

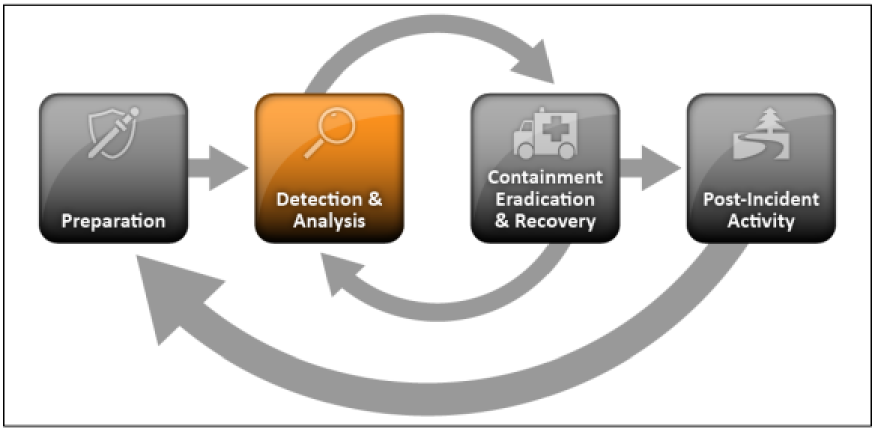


Figure 2.6: Detection & Analysis (Cichonski et al., 2012)

Attack detection can be done either manually or automatically. The discovery of an incident by an internal or external person is known as manual detection. Thus, security specialists such as analysts in the SOC or security novices can discover threats. An example of manual detection would be if an employee receives a phishing email and reports it so that the security team can take appropriate action (Vielberth et al., 2020).

Regarding automatic detection and analysis, the literature focuses on specific methods. Among detection methods, there are *anomaly-based* detection, *signature-based* detection and *specification-based* detection. The former method uses normal system behavior as a basis to distinguish and detect deviations (Vielberth et al., 2020). Triggering alerts when observed events differ from normal events (Bhatt et al., 2014). Signature-based detection uses a knowledge base of previous attacks and is useful to detect known threats of known system vulnerabilities. The latter method uses predefined profiles and protocols to detect incidents. For example by specifying known IOCs, you can tell the system to look for programs that behave according to the specification (Vielberth et al., 2020).

Containment, eradication & recovery

Following or during the detection and analysis phase, depending on the incident, a main objective is to be able to rapidly react and contain the incident, minimizing damage (Muniz et al., 2015).

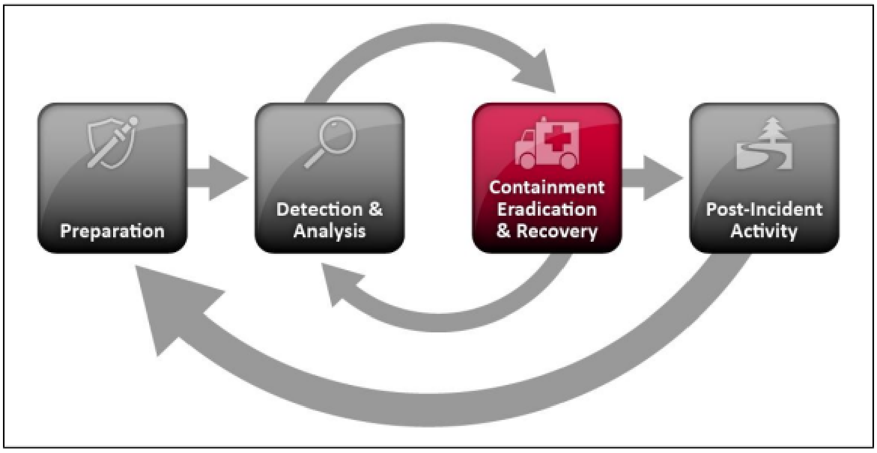


Figure 2.7: Containment, Eradication & Recovery (Cichonski et al., 2012)

Before an incident depletes resources or increases damage, it is essential to contain the incident, segregating or isolating it from the rest of the system (e.g., so that it cannot spread). Because most incidents require containment, this is an important consideration early in the course of incident handling (Cichonski et al., 2012). The SOC team typically has somewhat limited knowledge of the network and how data actually flows through it, and thus to manage the containment, eradication and recovery phase of an incident, systems and database administrators are almost always brought in and involved (Muniz et al., 2015).

An important consideration is decision-making, an essential component of containment (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures in place for dealing with the incident. Containment strategies differ depending on the incident type. For example, the strategy for dealing with an email-borne malware infection differs greatly from that of dealing with a network-based DDoS attack. Organizations should develop distinct containment strategies for each major incident type, with criteria clearly documented to inform decision-making (Cichonski et al., 2012). On this point it is important that the SOC knows to triage and escalate an incident in time, so that those decisions can be made.

Post-Incident Activity

In the systematic study by Vielberth et al. (2020), they emphasize that no SOC-specific scientific publication deals with the topic of "post-incident activity". Because of this, they did not consider the topic in their description of SOC processes, deeming literature incomplete. Considering Vielberth et al. (2020) reviewed 158 academic publications, having analysed 208 papers from 7 renowned databases we recognize there is a gap in existing literature about SOC operations. In an attempt to contribute to filling this gap, we have explored and enquired about the fourth step of the incident response cycle within SOCs through our empirical findings and discussion (Chapters 4.2.5 & 5.1.4). However, as you may recall, a *CSIRT* can be characterized as a stand-alone unit or as part of a SOC. Thus, we assume post-incident activity within CSIRTs to be similar or the same as that of SOCs;

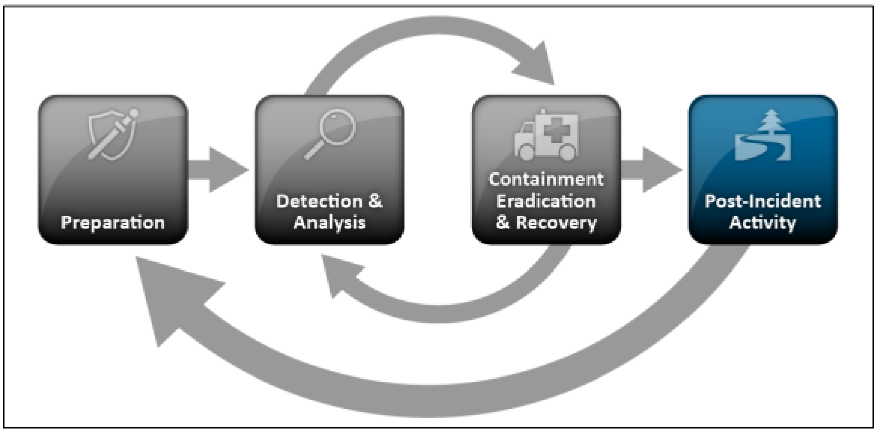


Figure 2.8: Post-Incident Activity (Cichonski et al., 2012)

One of the most important aspects of incident response is also one of the most frequently overlooked: learning and improving (Cichonski et al., 2012). This is where incident response teams seek to improve the incident response process and reflect upon the people, processes and technologies involved (Muniz et al., 2015). Conducting a "lessons learned" meeting with all parties involved following a major incident, and optionally after minor incidents as resources allow, can be extremely beneficial in improving security operations and the incident handling process itself. A lessons learned meeting provides an opportunity to bring an incident to a close by reviewing what happened, what was done to respond, and how well the response performed(Cichonski et al., 2012). It allows for reflection on the incident handling performance where 'lessons learned' are incorporated into standard operating procedures (Ahmad et al., 2021). The meeting should take place within a few days of the incident's ending. Other aspects of the *post-incident activity phase* involves using the collected incident data to e.g., conduct risk assessments; preserve evidence for prosecution of perpetrators; and storage capacity handling (how long certain types of data is kept from an incident)(Cichonski et al., 2012)

For security teams to manage and comply to all of these processes, and maybe more so the preparation and detection & analysis phases, modern enterprise SOCs are hierarchically structured around SIEM systems (Bhatt et al., 2014).

2.4 Security Information and Event Management (SIEM)

Among a SOC's goals are to monitor security related events from the enterprises' technology environments, including the IT network perimeter defense systems such as application servers, firewalls, databases, intrusion prevention devices, and user accounts. Each asset might be monitored using a variety of sensors and maintain log files of activity. The SOC receives event information from the sensors and log files and triggers alerts indicating possible malicious behavior, both at the perimeter of the network and in the enterprise.(Bhatt et al., 2014). In the wake of advanced security invasions, SIEM has replaced the Intrusion Detection and Prevention System (IDPS) to fulfill these goals (Chopra and Mahapatra, 2019). SIEM systems are an important tool used in SOCs as they collect security events from many diverse sources in enterprise networks, standardize the events to a common format, store the conformed events for forensic analysis, and correlate the events to identify malicious activities in real time (Bhatt et al., 2014). They have evolved into comprehensive systems that provide a broad view of high-risk areas and proactively focus on mitigation measures aimed at lowering incident response costs and time (González-Granadillo et al., 2021).

Despite the fact that the new generation of SIEMs offers powerful features in terms of correlation, storage, visualization, and performance, as well as the ability to automate the reaction process by selecting and deploying countermeasures, current response systems are severely limited, and countermeasures are selected and deployed without a thorough impact analysis of attacks and response scenarios (González-Granadillo et al., 2021). SIEM systems' main strength however, is their ability to cross-correlate logs from diverse sources using common attributes to define meaningful attack patterns and scenarios, which when they occur, can alert SOC analysts. Figure 2.9 illustrates a SIEM system's basic architectural components.

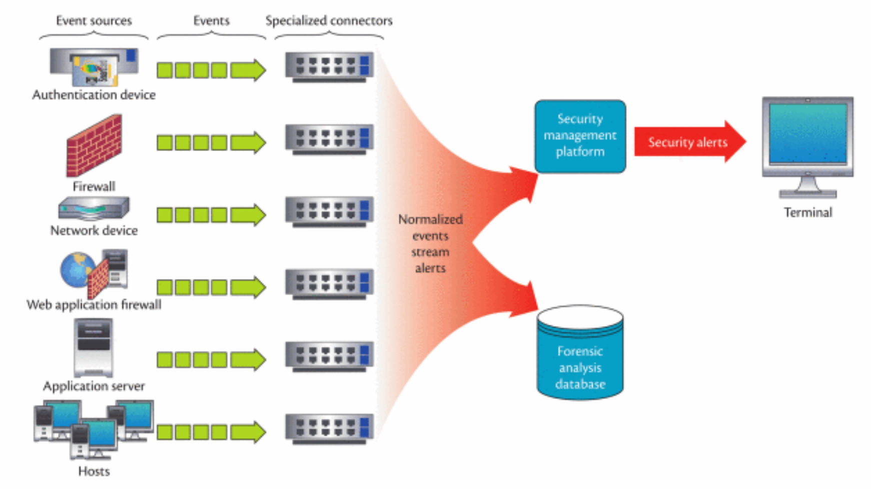


Figure 2.9: A typical SIEM system architecture (Bhatt et al., 2014)

The SIEM accepts input from various security devices and sensors including perimeter defense systems, applications, host- and network sensors. Each device and sensor is configured to output security events with unusual or anomalous behavior that might indicate malicious intent. These events may each be represented in different formats. Thus, the SIEM system's first task is to standardize the different representations into a normalized format to ease further processing and to simplify maintenance and rule creation. As the figure depicts, SIEM system connectors–customized for each source– receive the events. The connectors then parse the input events and convert them into a standardized format, and do so in a scalable manner to keep up with the event source. Once the events are conformed in a standardized format, they are forwarded to the security management platform and the forensic analysis database (Bhatt et al., 2014). All discovered anomalies/alerts are then ranked and shown in the SIEM dashboard. From this view, the system will send automated notifications to the right people, conduct automated corrective steps, and generate reports for management and key performance indicator (KPI) review on a regular basis (Podzins and Romanovs, 2019). Data analysts examine each anomaly separately after they've been discovered. If a false positive is discovered, the SIEM architect/content author or anyone else in charge of rule fine-tuning will optimize the rule that was triggered. If the anomaly constituted a legitimate security event, the relevant incident response workflow inside the SOC will be triggered.

The management platform's rule engine applies its rules periodically to a bulk of events, typically those captured in the last few hours. Whenever a rule triggers a new alert, the alert is sent to the SIEM platform terminal for analysis by the SOC. Each rule captures information about malicious behavior. For example, a rule might look for suspicious login attempts within a time window or look for HTTP requests to known malicious URLs. The rules are generated from two sources: a SOC engineer can create rules, and the SIEM system can algorithmically generate rules from events, e.g., via pattern mining - that is, identifying sets of events that occur together frequently within a time frame. A rule engine might also be configured with anomaly detection - triggering alerts when observed events differ from normal events (Bhatt et al., 2014). A single event may not trigger an alarm in some cases though, but a consistent pattern would. The internal rules engine of the system does this. Systems require ongoing optimization, which is one of the most serious issues. Artificial intelligence modules are available from most major SIEM vendors (Splunk, IBM, LogRhythm, etc.) and are designed to make analysis more "intelligent" by allowing it to adapt to changes in the environment. This component is still a long way from being a "set-up-and-forget" solution, but its effects are improving, and if properly optimized, it will increase overall anomaly detection efficiency (Podzins and Romanovs, 2019)

According to Podzins and Romanovs (2019), SIEM solutions have significant advantages and disadvantages, which are summarized in the table (2.3) below. We include the table for the purpose of highlighting a SIEM's applicability in a summarized format, in an attempt to create an overview of its usefulness.

Security Information and Event Management (SIEM)	
Advantages	**Disadvantages**
Centralized log storage - in the event that the primary log source is unavailable, a secondary log storage with high file availability, integrity, and confidentiality will always be available.	SIEM systems are costly; the initial purchase price, which includes license costs based on the volume of logs processed/indexed, will be prohibitively expensive if log files are not prioritized.
Increased incident response efficiency.	SOC will be required 24 hours a day, 7 days a week, which will significantly increase the costs (mostly on salaries).
Will be able to acquire a "big picture" of what is going on in the IT environment at any given time.	If you're not careful, the amount of maintenance required to examine alarms and improve SIEM (fix "False Positives") can rapidly become overwhelming.
Forensic information on historical events. At the same time, audit log integrity is maintained.	Employees to configure and use the system is expensive, hard to hire (because of security knowledge shortage in the market) and even harder to hold them.

Table 2.3: Advantages and disadvantages with SIEM

> "*State-of-the-art SIEM is undoubtedly the enabling technology of a modern effective security operations centre (SOC). Before SIEM, security professionals were essentially blind, unable to see what was happening in their own IT environments*" (Gailey, 2020).

While SIEM systems provide control over networks and systems, to be able to gain a knowledge advantage over cyber threat actors and anticipate potential threats and risks, SOC personnel needs to 'raise their gaze' and look into the operational environment and the current threat picture. Bhatt et al. (2014) makes the point that, among many dependencies, a SOC's effectiveness depends on its access to actionable threat intelligence.

2.5 Cyber threat intelligence (CTI)

The volume of cyber attacks and malware varieties has risen significantly in recent years, making it increasingly challenging for security analysts and forensic investigators to discover and protect against cybersecurity threats. To address this issue, researchers coined the term *"Threat Intelligence"* which refers to *"the set of data collected, assessed and applied in relation to security threats, threat actors, exploits, malware, vulnerabilities, and compromise indicators."*(Conti et al., 2018). CTI provides knowledge of a malicious actor's capabilities, infrastructure, motives, goals, and resources in cyberspace (Jasper, 2016). In fact, CTI was established to support security practitioners in recognizing the indicators of cyber threats, extracting information about the attack techniques, and, as a result, accurately and swiftly responding to the attack (Conti et al., 2018). The primary goal of CTI is to gain a knowledge advantage over cyber threat actors. CTI accelerates the detection of malicious behavior at the tactical and operational levels, ideally before a malicious actor gains a foothold in the network. On a Strategic level, CTI helps decision-makers make sense of and gain insight into the relevant threat environment (Oosthoek and Doerr, 2021). The use of threat intelligence enables an organization to prioritize defenses around prized assets, focusing on vulnerabilities and ways that an adversary activity can be mitigated (Jasper, 2016). Wagner et al. (2019) consequently states that CTI is not simply information, it is information that has been analyzed and is actionable.

It is becoming increasingly necessary for organizations to have a cyber threat intelligence capability and a key element of success for any such capability is information sharing with collaborators, peers and others they select to trust (Barnum, 2014). While cyber threat intelligence and information sharing can assist companies in focusing and prioritizing the use of the substantial quantities of complicated cyber security data they encounter today, they still require standardized, structured representations of this data to make it tractable. This relates to how organizations and cybersecurity stakeholders exchange information.

2.5.1 Information exchange

Reducing cybersecurity risk by enhancing cyber situational awareness in organizations increasingly depends on information sharing and collaboration among a wide range of actors, leveraging many different models, methods, and mechanisms. As reported by Goodwin et al. (2015), information sharing is the process of sharing information about cybersecurity incidents, threats, vulnerabilities, best practices, mitigation measures and other topics. Wagner et al. (2019) explains that sharing of CTI is an effective way of enhancing the situation awareness of an organization and its stakeholders. Moreover, it is seen as a necessity to survive current and future attacks by working proactively instead of only reactive. It may become obligatory for organizations to have a threat intelligence program and disclose their knowledge as part of proactive cyber security. Stakeholders may be held responsible in the future for not sharing known threats that could affect others resulting in a breach. The core idea behind threat intelligence sharing is to create situation awareness among stakeholders through sharing information about the newest threats and vulnerabilities, and to swiftly implement the remedies(Wagner et al., 2019).

The Structured Threat Information eXpression (STIX) is a community-driven initiative to define and develop a language to describe structured threat information (Barnum, 2014). STIX is an expressive, flexible, and extensible representation language used to communicate an overall piece of threat information (Sauerwein et al., 2017). According to a study of existing threat intelligence sharing initiatives, Sauerwein et al. (2017) concludes that STIX is the most used standard for sharing structured threat information. The architecture is comprised of several cyber threat informations such as cyber observables, incidents, indicators, adversaries tactics, procedures, techniques, exploit targets, courses of action, cyber attack campaigns, and threat actors (Barnum, 2014). To share this structured threat information, the most commonly used standard is TAXII (Trusted Automated eXchange of Indicator Information)(Sauerwein et al., 2017). TAXII is a collection of services and message exchanges to enable the sharing of information about cyber threats across product, service and organizational boundaries. It is seen as a "transport vehicle" for STIX structured threat information and a key enabler to widespread exchange. Both STIX and TAXII are products made by the Mitre Corporation (Mitre.org, 2022).

In cybersecurity, receiving the right information at the right time can empower decision-makers to reduce risks, deter attackers, and enhance resilience. Sharing the right information is more than people exchanging data, it is also about the automation of machine-to-machine sharing to counter fast-moving threats (Goodwin et al., 2015). Within the concepts of CTI management and especially information sharing, several authors (Leszczyna and Wrobel (2019); Ahmad et al. (2021); Naseer et al. (2021); Skopik et al. (2016)) promote the concept of inter-organizational sharing networks for exchange of threat intelligence information, primarily by the use of SOCs. This gives organizations a considerable advantage when fighting against cyber threats (Ahmad et al., 2021). Multiple studies, including de Fuentes et al. (2017) and van der Kleij et al. (2022) confirms that cooperative cyberdefense is as an essential strategy to fight against cyberattacks. Cybersecurity Information Sharing (CIS), especially about threats and incidents, is a key aspect in this regard, and according to the European Union Agency for Cybersecurity (ENISA), 80 initiatives and organizations and more than 50 national and governmental Computer Security Incident Response Teams (CSIRTs) are involved in CTI sharing at European Union (EU) and European Economic Area (EEA) level (Wagner et al., 2019). CIS provides members with an improved situational awareness to prepare for and respond to future cyber threats. Privacy preservation is critical in this context, since organizations can be reluctant to share information otherwise. This is particularly critical when CIS is facilitated through an untrusted infrastructure provided by a third party (e.g., the cloud).

Despite the obvious benefits, organizations appear to be hesitant to join information sharing networks. As reported by de Fuentes et al. (2017), organizations are not inclined to share cybersecurity intelligence (including ongoing or past cyber incidents) neither with governments nor with other partners or competitors. Reasons include the lack of trust in the sharing infrastructure, particularly if it is run by a potential competitor or adversary, and the way sharing is carried out. For example, in networks in which the government is involved, companies prefer to remain anonymous in case of incidents that uncover infringement of rules, i.e., leakage of unprotected personal data. Another concern as expressed by van der Kleij et al. (2022) is that professionals may sometimes have to deal with a large number of parties, of diverse backgrounds and using different professional languages, which by nature complicates the exchange of information especially in stressful situations. Wagner et al. (2019) consequently states that a prevalent reason why companies do not share their CTI is the belief that they have nothing worth sharing and that competitors will use the knowledge against them. It is unfortunate, because even if they believe the information is useless, it may be this information that prevents another organization from being compromised by improving their situational awareness.

2.6 Situational awareness

Situational awareness, often and hereby referred to as situation awareness or SA (for the sake of simplicity), is a multifaceted and well-studied phenomenon (Franke and Brynielsson, 2014). SA is from a technical point of view defined as the compiling, processing, and fusion of data. Such data processing necessitates the ability to evaluate data fragments as well as fused information and provide a reasonable estimate of its information quality (Arnborg et al., 2000). As a result, it is conceivable to technically relate and assess pieces of data in relation to one another. The *cognitive* component of situation awareness, on the other hand, is concerned with the human capacity to comprehend technical implications and draw conclusions in order to make informed decisions. Cognitively, it is thus interesting to assess to what extent a human decision-maker is aware of the situation, i.e., has reached a certain level of SA, and how well he or she manages to maintain and develop this awareness over time (Franke and Brynielsson, 2014).

In the following sections, we attempt to cover the many definitions that make up the subject of SA. With the purpose of uncovering 'the multiple facets' of the subject, we provide a background and theoretical lens to relate to throughout the project report.

2.6.1 Cybersecurity situation awareness

The widely applied and most common definition of situation awareness is that of Endsley (1995), which from a cognitive point of view defines SA as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*". Endsley (1995) describes SA as part of a larger process for human cognition that is framed from an information-processing perspective. It is apparent in the literature, that authors most of the time refer to and "translate" Endsley's conceptualization into their own perspective when defining SA in cybersecurity.

Evesti et al. (2017) states about SA in cybersecurity that "*building situation awareness requires capability to gather information from the environment, means to understand gathered information, and reflecting the gained understanding for the current environment*". Here - gather, understand and reflect are synonyms for perceive, comprehend and project. Furthermore, Ahmad et al. (2021) defines SA in IR as "*the perception of incident-related elements within the organizational environment over the course of the incident, the comprehension of their meaning within the context of the organization's cybersecurity mission and objectives, and the projection of their status in the near future*" - Here, the body of the definition is altered to fit the dynamics and attributes of organizational incident response perspective and environment. Consequently, Ahmad et al. (2021) offer a more comprehensible example, framing SA as "*a problem of collecting relevant and useful information (i.e. 'collect the dots'), fusing together key elements of the information (i.e. 'connect the dots') and deriving insights from the fused information ('project from the dots')*" - much like how Rajivan and Cooke (2017) compares SA to knitting pieces of a puzzle together. You collect the pieces ('the dots'), connect them and reflect upon the picture that emerges. Simultaneously, collecting and connecting the pieces of the puzzle are synonyms for perceiving and comprehending, while the finished puzzle represents insight of the environment of which an operator can reflect upon (projection) to inform decision-making. Moreover, Franke and Brynielsson (2014) adds, based on the conceptualization of Endsley that "*the words "perception", "comprehension", and "projection" within cybersecurity can be taken to denote progressively increasing awareness levels ranging from (i) basic perception of important data, (ii) interpretation and combination of data into knowledge, and (iii) the ability to predict future events and their implications*".

By these multiple definitions and perspectives we develop an understanding of the overall meaning of SA and its transferable meaning to SA in cybersecurity. Proceeding from Endsley's definition, *Perception* may in cybersecurity terms incorporate the gathering of useful and important incident-related data or collecting of cybersecurity information from the organizational environment over the course of an incident. Comprehension is about understanding; interpreting and combining that data into usable knowledge and intelligence within the context of the organization's cybersecurity mission and objectives, and *Projection* involves the reflecting of the gained understanding for the current environment, deriving insights from the processed data to predict future events and their implications.

Additionally, on a side note, there is the concept of '*team* situation awareness' or team SA. Endsley (1995) defines this, from a human-centered point of view, as "*the degree to which every team member possesses the SA required for his or her responsibilities*". Largely applicable to the cybersecurity SOC and IR processes (a team effort), Rajivan and Cooke (2017) describes the concept as members of a team becoming aware of different aspects of a situation and *knitting the pieces of the puzzle together* through communication or other interactions to achieve team SA and to take appropriate action. The implementation of team SA as a concept makes sure every team member is adequately informed and aware to make the best decisions, collectively and across knowledge-areas in a fast-paced environment.

2.7 Theoretical lens

The theoretical lens is how we choose to interpret the phenomena that we investigate in our study, as there are several theories and approaches in the study of situation awareness. As may be apparent, the theory of Endsley (1995) which takes an information processing approach is the most dominant, as it is repeated in existing literature about the subject. As a basis for this study, this is the selected theoretical lens. However, Endsley (1995) writes about general SA within an *objective operator*'s perspective, and does not specifically focus on SA in cybersecurity. A more recent study by Ahmad et al. (2021) on the other hand, addresses this issue and provides a definition of SA in cybersecurity IR specifically; *"the perception of incident-related elements within the organizational environment over the course of the incident, the comprehension of their meaning within the context of the organization's cybersecurity mission and objectives, and the projection of their status in the near future"*. Drawing on this definition, the result is a bilateral theoretical lens, which takes basis in Endsley (1995)'s conceptualization of the situation awareness process, incorporating Ahmad et al. (2021)'s point of view. Along with the definition of SA in cybersecurity, we base our study on certain models and flow diagrams as you will see throughout this section, which set the basis for our coming conceptual framework.

2.7.1 Situation awareness of the environment

Figure 2.10 below illustrates Endsley (1995)'s situation awareness process model for human cognition that is framed from an information-processing perspective. Here, 'Situation Awareness' (bold outline box) is an operator's 'state of knowledge' that can exist at three different level states – perception, comprehension and projection. The three states of SA collectively lead to the making of a decision and subsequently the execution of action. Finally, the interaction of the operator with the real-world environment (feedback) results in further modification of the operator's mental model which again directs further actions (Ahmad et al., 2021). Within a SOC environment, the operator most of the time is a SOC analyst, but could also be a major incident team, of which we will come back to later (but keep that in mind as you read about the operator throughout the next section).
Within the *Situation Awareness* process, *Perception* is a state of knowledge that reflects the operational picture of the environment (Ahmad et al., 2021). The *Environment* includes the status, attributes, and dynamics of elements in the operational domain relevant to the operator. E.g., a pilot would perceive elements such as aircraft, mountains, weather or warning lights along with their relevant characteristics (e.g., color, size, speed, location) (Endsley, 1995). I.e., perception results from the gathering of raw data through actions such

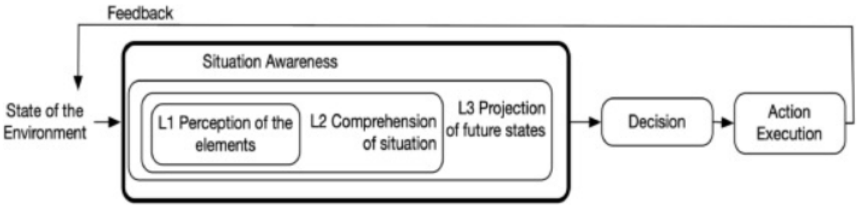

Feedback
Situation Awareness
State of the Environment
L1 Perception of the elements
L2 Comprehension of situation
L3 Projection of future states
Decision
Action Execution

Figure 2.10: Situation Awareness (Adapted from Endsley) (Ahmad et al., 2021)

as sensing the environment, interacting with the environment or even receiving messages from the environment (Ahmad et al., 2021). For example, operators may develop insights using visualisation *to sense the environment*; employ tools to structure this insight to allow for *interaction with the environment* (e.g. in ways that instruct computers to conduct future work for them); or receive alerts from e.g. sensors that requires human interpretation, *acquiring messages from the environment* (Conti et al., 2013). *Comprehension* is a higher level state of knowledge resulting from the operator processing key elements from the operational picture into their mental model so the significance of the elements to the operator's objectives and mission become apparent (Ahmad et al., 2021). Franke and Brynielsson (2014) explains this as the fusion of data, i.e. the data used to develop SA is the result of data fusion. Simply put, fusing raw data into comprehensible information for developing decision support systems that ultimately serve to help a decision-maker gain and further develop a high degree of SA. *Projection* is the third and highest level state of knowledge. It results from the operator extrapolating from their existing mental model to produce plausible states of the system and the environment in the future (Ahmad et al., 2021). For example by conducting risk analysis and recognizing business critical assets and processes to adapt countermeasures to better suit the current and future environment (Evesti et al., 2017). Projection is purposeful and supports goal-oriented decision-making; the operator assesses the situation and interprets what might or will happen in the future in the context of its objectives and mission as a basis for future decision-making (Ahmad et al., 2021).

Decision and *Action Execution* are stages that are separate from the *Situation Awareness* process but follow from it as part of the larger process model of human cognition (Ahmad et al., 2021). Hence, SA exists as a facilitator for decision-making rather than part of it. I.e., SA is produced as input for decision-makers deciding how to react to a situation (Evesti et al., 2017). Thus, the Decision-stage is where the operator makes a course of action based on the SA knowledge constructed during the *Situation Awareness* process. Consequently, Action Execution is where the operator puts the decision into effect based on the previous stage to continuously change the state of the environment (Ahmad et al., 2021). This decision or choice of action leans on strategical SA knowledge constructed in the projection state relative to Endsley's cognitive model (Evesti et al., 2017). The final stage (feedback) imposes the course of action and impacts the real world which is ultimately perceived by the operator through its *Situation Awareness* all over again (Ahmad et al., 2021).

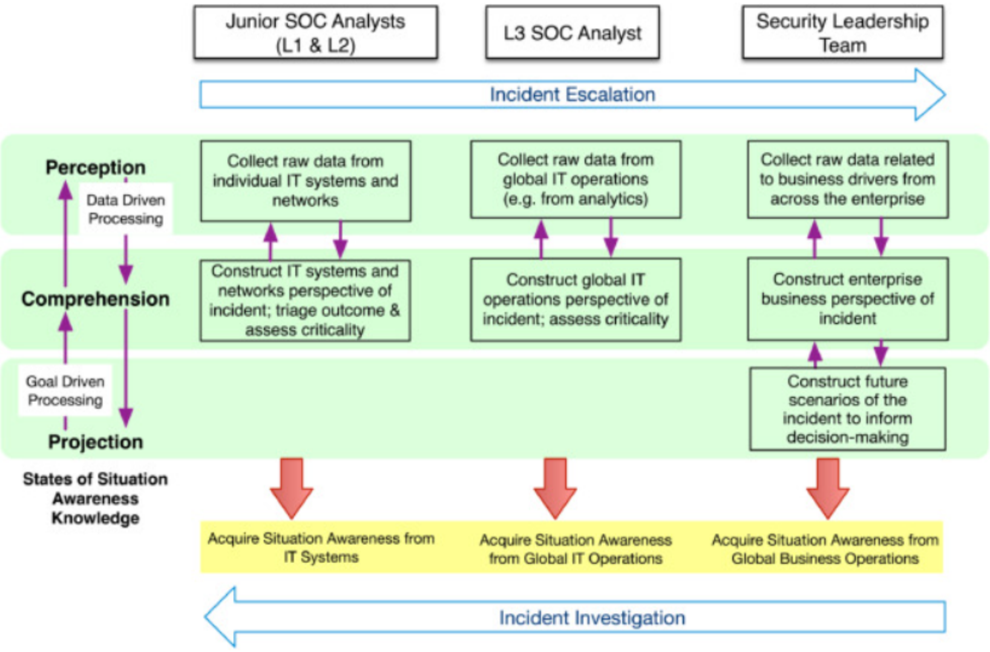
2.7.2 Situation awareness in cybersecurity IR

A case study by Ahmad et al. (2021) on the management practice of organizational incident response contributes a process model of SA in cybersecurity IR (Figure 2.11). In their study, they suggest that SA is a critical attribute of organizational IR and answer "How can organizations practice situation awareness in incident response?"

As a result, they identified three key ingredients required for a process model of SA in cyber IR.

- The stakeholders
- The process inputs (playbooks, mental models, strategic, business and IT context, and threat intelligence
- The process outputs (perception, comprehension, and projection)

To understand how teams of security operations perceive, comprehend and project SA knowledge and dynamically behave to manage enterprise detection and response, this model is our point of reference. In this section we break down the model to explain its processes.



Junior SOC Analysts (L1 & L2)
L3 SOC Analyst
Security Leadership Team
Incident Escalation
Perception
Data Driven Processing
Comprehension
Goal Driven Processing
Projection
States of Situation Awareness Knowledge
Collect raw data from individual IT systems and networks
Collect raw data from global IT operations (e.g. from analytics)
Collect raw data related to business drivers from across the enterprise
Construct IT systems and networks perspective of incident; triage outcome & assess criticality
Construct global IT operations perspective of incident; assess criticality
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Acquire Situation Awareness from IT Systems
Acquire Situation Awareness from Global IT Operations
Acquire Situation Awareness from Global Business Operations
Incident Investigation

Figure 2.11: Situation Awareness in Cybersecurity IR (Ahmad et al., 2021)

The process model is represented in two dimensions. The green boxes on the horizontal dimension is used to model cybersecurity stakeholders. The vertical dimension represents SA as of Endlsey's three states of cognition (perception, comprehension, and projection). There are two types of dynamic behavior in the process model. The first is task behavior (investigation vs. escalation), and the second is information processing behavior (goal-driven vs. data-driven) (Ahmad et al., 2021).

The purple arrows in Figure 2.11 represent information processing behavior by allowing progression across the three states of SA knowledge. The purple arrows pointing downward indicate that data-driven processes can help organizations achieve increasingly higher levels of SA (moving from perception to comprehension to projection). The upward pointing purple arrows between the states indicate that goal-driven processing, such as attention-focusing, result in lower levels of SA utilizing existing mental models (moving from projection to comprehension to perception) (Ahmad et al., 2021).

Each stakeholder's contribution to SA is characterized in terms of their frame of reference (yellow bar). In comparison to senior SOC analysts, junior SOC analysts have a limited frame of reference. Individual IT systems and networks within the organization are the focus of their efforts. Analysts at L3 SOC have a broader perspective that includes the company's global IT operations. The Security Leadership Team, which covers the entire company, has the largest frame of reference. Their perspective is business-centered rather than technology-centered, which is a key distinction (Ahmad et al., 2021).

The processes of SA run continuously, in parallel, and can be data-driven and goal-driven at the same time (Ahmad et al., 2021).

Levels of Situation Awareness

Evesti et al. (2017) divides the goal of SA into two level categories of operational and strategic, concentrating on SA from temporal and decision-makers position perspectives. Here, SA can be seen as short-term day-to-day operational information or long-term strategical information. Ahmad et al. (2021) provides a similar insight towards the operational and Strategic levels of SA in cybersecurity, but adds on the tactical level, including the roles responsible for each level of producing SA information and perspective as you can see in figure 2.12.

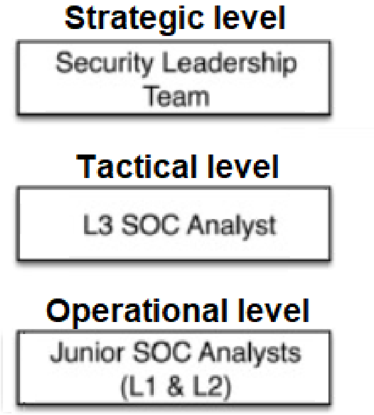


Figure 2.12: Levels of SA (grounded in theory of (Ahmad et al., 2021))

Operational level SA produces information for short-term decision making. In other words, data is collected mostly in real time, and analysed on daily or weekly basis. The operational level SA is built by level 1 and 2 junior SOC analysts applying various monitoring and analysis tools and alerts at different priorities from immediate to near-short term (Evesti et al., 2017; Ahmad et al., 2021). Here, the analysts apply playbooks, mental models, tacit knowledge about the organization and incident, and operational threat advice to synthesize incident-related elements within their existing knowledge, for triage and criticality assessment (Ahmad et al., 2021).

Tactical level SA produces tactical intelligence which involves hypothesizing about threat activity impacting the enterprise and validating that against the observations of tactical level analysts. The tactical level can be viewed as an additional level within the operational level as described by Evesti et al. (2017), or rather a higher level - between the operational level and Strategic level as you can see in Figure 2.12. Here, more qualified/senior level (tier 3) analysts oversee and draw on analytics-driven reporting from lower-level analysts (at the operational level) and make decisions based on a more mature mental model (more experienced and goal oriented). Their mission is to synthesize incident-related elements within their existing knowledge for sense-making and further criticality assessment (Ahmad et al., 2021).

Strategic level SA produces long-term information for executive decision-makers. The produced SA is utilised to define, e.g., policies, which in turn is reflected to the whole organisation. Moreover, Strategic level SA, risk analysis and recognition of business critical assets and processes are central tasks. Hence, the protected assets, which relate to enterprises main objectives and business operations, have to be identified in the Strategic level. Furthermore, threats and vulnerabilities towards these assets have to be recognised. Strategic level SA, produced by risk analysis, makes it possible to define required high-level security controls and an acceptable risk level (Evesti et al., 2017). Here, the security leadership team apply mental models, tacit knowledge, and input about strategic business context to synthesize incident-related elements with existing knowledge for the purposes of understanding (comprehension of the situation). With the most equipped mental models, the leadership team apply strategic threat advice to generate future scenarios of the incident to inform decision-making (Ahmad et al., 2021).

2.7.3 Information flow and communication pathways in IR

In the study by Ahmad et al. (2021), they present an illustration of the information flow and communication pathways in SOC-IR within the anonymized enterprise "FinanceCentral". The figure below (Figure 2.13 depicts this illustration. The model shows the dynamics of the case organization, and how information flow and communication pathways flow through the different technologies and people. Using this insight, we can understand how teams of security operations really function in incident response from the technology components which allows for the perception of elements in the environment to the Security Leadership Team (SLT) which projects the acquired SA to eventually make a decision.

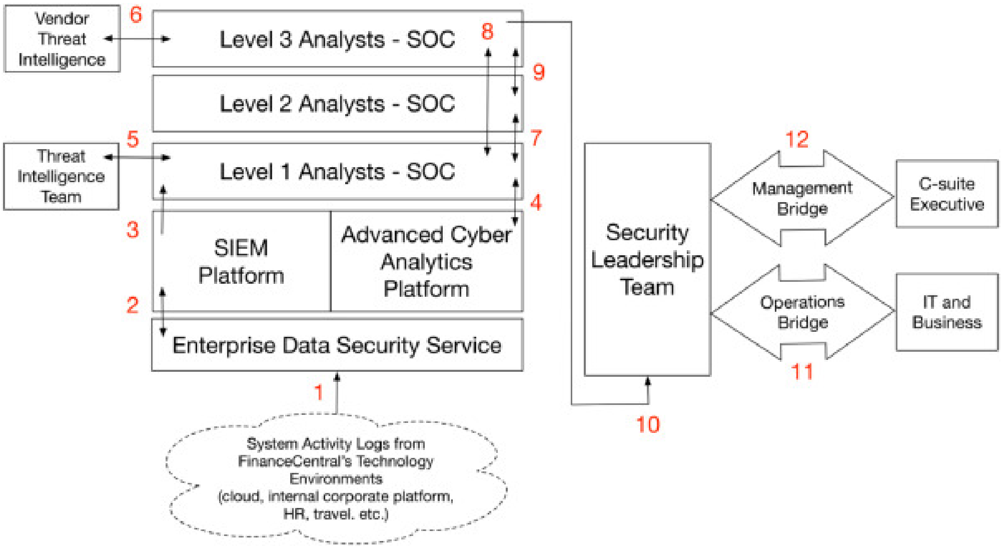

Vendor Threat Intelligence
6
Level 3 Analysts - SOC
8
9
Level 2 Analysts - SOC
7
Threat Intelligence Team
5
Level 1 Analysts - SOC
4
3
SIEM Platform
Advanced Cyber Analytics Platform
2
Enterprise Data Security Service
1
System Activity Logs from FinanceCentral's Technology Environments (cloud, internal corporate platform, HR, travel. etc.)
Security Leadership Team
10
12
Management Bridge
C-suite Executive
Operations Bridge
11
IT and Business

Figure 2.13: Information flow and communication pathways in IR (Ahmad et al., 2021)

The Level 1 security analysts collect raw data from the *SIEM platform*. The information flow from the SIEM platform to the analysts (arrow 3) describe how SA of the environment is perceived through the SIEM. Before reaching the analysts, the SIEM platform collects its raw data from *System Activity Logs* obtained from the *Enterprise Technology Environments* (arrow 1) through the *Enterprise Data Security Service* (arrow 2). Thus, the SIEM is the focal point of which the SOC relies on to be able to do their job. The *Threat intelligence team* provides threat intelligence to the different stakeholders of the organization. At an operational level, the team monitor the threat landscape and feeds actionable intelligence to L1 analysts, another means of constructing SA of the environment. Consequently, the security analysts communicate across the SOC axis to convey actionable data and perspectives of an incident as it potentially escalates, requiring increasing levels of SA knowledge as we have learned from the process model and the explanation of the different levels; operational, tactical and strategic. On a Strategic level, the organization pays for a vendor of threat intelligence which provide a direct line to expert analysts and ready-made CTI of which they can draw on in need, during a major incident (arrow 6). A major incident triggers the formation of the security leadership team (arrow 10). One of the SLT's responsibilities in such a situation is to open communication channels to relevant stakeholders, and direct the incident response. To execute these responsibilities the SLT initiates a formal 'managed incident' process which comes with a dedicated technical incident recovery manager. The team through the recovery manager set up two communication platforms, of which they call bridges. One management bridge and one operational bridge. With the former channel, the SLT communicate with C-suite executives; through the CISO with the senior executive of the organization. This communication is critical to rapid decision-making and coordination. Through the operational channel, the SLT coordinates communication with the IT and business domains of the organization, including leaders and stakeholders of the technology domains relevant to contribute with the enterprise response (Ahmad et al., 2021).

Drawing on the knowledge constructed from this and the previous models and explanations, a coherence becomes apparent of which constructs the theory-informed narrative that comprises our theoretical lens. Following chapter 3 we present our conceptual framework in the result chapter which reflects this coherence.

Chapter 3

Research approach

The purpose of this exploratory study is to develop an understanding of the concept of situation awareness and its relation to cybersecurity; investigate its function in the context of enterprise MSSP security operations and examine how situation awareness knowledge is constructed through the organizational levels of the enterprise response. To accomplish this, the study addresses two research questions (RQs):

- (RQ1) How are leading Managed security service providers (MSSP) operationalized to provide security operations as a service?"
- (RQ2) "How is situational awareness knowledge constructed through the organizational levels of the MSSP?"

This chapter presents arguments for why the chosen research approach and its philosophical assumptions is suitable for the project and argues for why the alternative research approach is considered less suitable.

3.1 Qualitative approach

Qualitative approach in information systems research is a broad umbrella term that covers a wide range of techniques ranging from interviews, observational techniques such as participant observation and fieldwork, through to archival research (Hennink et al., 2020; Myers, 2021). In qualitative research, philosophical assumptions include interpretive and naturalistic approaches (Hennink et al., 2020). Qualitative research 'involves an interpretive, naturalistic approach to the world. This means that qualitative researchers study things in their natural setting, attempting to make sense of, or interpret phenomena in terms of the meanings people bring to them'(Denzin and Lincoln, 2008). Some sources claim qualitative research can also be positivist and critical, meaning building an understanding of phenomena through theory testing building on hypotheses and, respectively, that social reality is historically constituted and that it is produced and reproduced by people (Myers, 2021). Situational awareness in cybersecurity however, is in our opinion rather not (particularly) historically constituted and neither easily hypothesized as it requires a unique subjective enterprise context to be examined. Thus, the position of interpretivism in relation to ontology and epistemology is that interpretivists believe that reality is socially constructed, assuming that access to reality is only through social constructions such as language, consciousness and shared meanings (Myers, 2021). Fittingly so, as Walsham (1993) p.4-5 quotes; *'interpretive methods of research in IS are "aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context"'*. Relating Walsham (1993)'s quote to our study, one could say that this IS research is "aimed at producing an understanding of the context of the SOC, and the process whereby the SOC influences and is influenced by SA in cybersecurity". We find that the advantages of conducting qualitative research allow us to have an increased degree of flexibility in the research design; the ability to avoid reliance on the researcher's predetermined assumptions; the opportunity to provide greater depth and detail in a researcher's findings; and the capacity to simulate participants' unique individual experiences (Griffin, 2004).

We selected a qualitative approach with interviews as it allows participants elaborate in ways that are not possible with other methods like survey research. Depending on how willing the interviewee is to share information on how they operationalize security operations to i.a construct situational awareness, it is believed that a qualitative approach would be an ideal option. However, qualitative data analysis is not always an easy and straightforward task. It is up to every researcher how to do the analysis, as there are no hard and fast rules about how to do it. Whereas quantitative data analysis can bring well-established mathematical and statistical procedures, qualitative research allows for more in-depth analysis. Qualitative analysis is more dependent on the skill of the researcher to see patterns and themes within the data (Oates, 2006). Focusing on opportunities, it would be important to establish a good and well thought-through interview guide.

> "*Qualitative research methods are designed to help researchers understand people and the social and cultural context within which they live. The goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context is largely lost when textual data are quantified*" (Myers, 2021).

To justify our choice of research approach, we have included a comparison of qualitative research and quantitative research from the book "Qualitative Research Methods" where Hennink et al. (2020) address the key differences (see table 3.1).

	Qualitative research	**Quantitative research**
Objective	To gain a contextualized understanding of behaviours, beliefs, motivation	To quantify data and extrapolate results to a broader population
Purpose	To understand why? How? What is the process? What are the influences or contexts?	To measure, count, or quantify a problem. To answer: How much? How often? What proportion? Which valiables are correlated?
Data	Data are words (called textual data)	Data are numbers (called statistical data)
Study population	Small number of participants; selected purposively (non-probability sampling) Referred to as participants or interviewees	Large sample size of representative cases Referred to as respondents or subjects
Data collection methods	In-depth interviews, observation, group discussions	Population surveys, opinion polls, exit interviews
Analysis	Analysis is interpretive	Analysis is statistical
Outcome	To develop an initial understanding, to identify and explain behavior, beliefs or actions	To identify prevalence, averages and patterns in data- To generalize to a broader population

Table 3.1: Qualitative VS Quantitative aspects (Hennink et al., 2020)

By looking at the table above, it is apparent to us that a qualitative approach would be a better fit for our research project. Considering the objective and purpose of this research study; what information we want, and what method that can provide it. Referring to Table 3.1, the purpose of this study is not to measure, count or quantify a problem, nor is the objective or outcome to identify patterns in data. It is rather to develop an understanding and an explanation of the 'behavior and actions' of SOC operators in the context of their typical organization, and to understand "why", "how" and "what is the process" of something, which is in the nature of this exploratory study.

3.2 Research Design

The choice of research design relates to the nature of the research problem and the type of knowledge information required to answer the research questions (Cresswell, 2008). The goal of this study is to investigate and gain a better understanding of the concept of situation awareness and its relation to cybersecurity; investigate its function in the context of enterprise MSSP security operations and examine how situation awareness knowledge is constructed through the organizational levels of the enterprise response; As we have already covered under 3.1, Myers (2021) makes the point that an interpretive qualitative approach within IS research are aimed at producing an understanding of the context of the *information system*, and the process whereby the *information system* influences and is influenced by the context. This identifies well with our approach, and implies the position of our research design. Our aim is to produce an understanding of the SA and its relation to cybersecurity and investigate its function in the context of security operations. Meanwhile, Sarker et al. (2018) states that "analysis within *exploratory studies* often involve (...) *induction* by engaging in some common-sense way of developing an accurate picture of a situation and its implications, which generates claims in the form of a *new framework*, propositions, or lessons learned". This appropriately also relates well with our case, as our objective is to develop - exactly - a new framework portraying how SA is operationalized and constructed through different organizational levels of enterprise MSSP's (ref. RQs). Thus, our research may also imply the position of inductive exploratory research.

To resolve this ambiguity - among genres within qualitative research, Sarker et al. (2018) presents a map (figure 3.1 below) of prominent qualitative approaches adopted in the IS community.

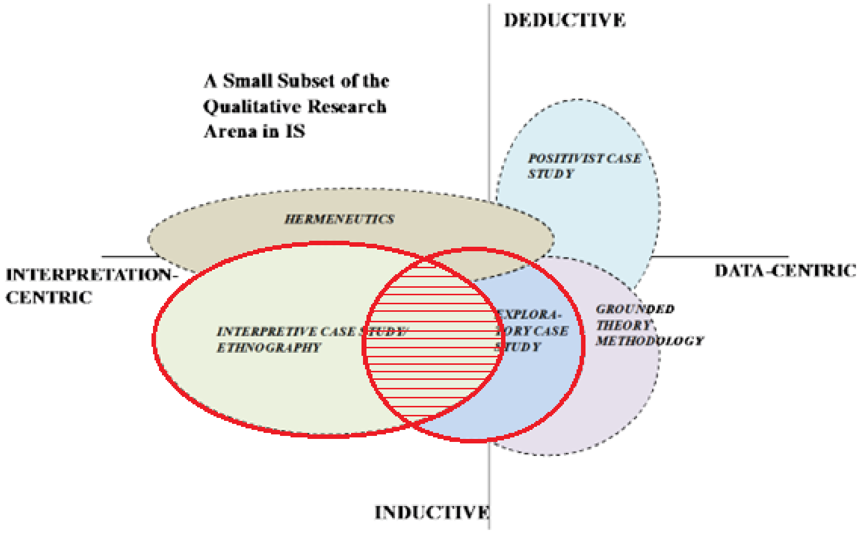

DEDUCTIVE
A Small Subset of the Qualitative Research Arena in IS
POSITIVIST CASE STUDY
HERMENEUTICS
INTERPRETATION-CENTRIC
DATA-CENTRIC
INTERPRETIVE CASE STUDY/ ETHNOGRAPHY
EXPLORA-TORY CASE STUDY
GROUNDED THEORY METHODOLOGY
INDUCTIVE

Figure 3.1: A Map of Genres in Qualitative Research (Sarker et al., 2018) (redacted)

In the search to distinguish the approaches of interpretive and exploratory studies, to position our research study, we identified an overlap between the two approaches in question (red striped area). Thus, we argue that this is an exploratory study - bringing elements from the interpretive tradition - i.e., by interpretive we a) construct a theory-informed narrative using a theoretical lens (Endsley's theory) (2.7) to b) produce an iterative understanding with a "hypothesis" (conceptual framework) followed by "validation" (Sarker et al., 2018) (interviews) to produce the final validated framework. As can also be seen in Figure 3.1, the two approaches lean most-of-all towards *inductive* reasoning (bottom dimension). This is best described by Given (2008) in *The SAGE Encyclopedia of Qualitative Research Methods* as "*a form of reasoning used in pursuit of understanding and knowledge, establishing a relationship between observations and theory*". In this respect, we argue that we observe through the experiences of the practitioners who are the ones who perform cybersecurity tasks on a daily basis. Through interviews we get first hand information about their activities, establishing a relationship between *observations* and theory. The result is that this is an inductive exploratory study with elements from the interpretive tradition of qualitative research.

3.3 The unit of analysis and subject selection

This exploratory study aims to examine how leading Managed security service providers (MSSP) are operationalized to provide security operations as a service while catering to the needs of situational awareness. A MSSP provides outsourced monitoring and management of security devices and systems. Common services are managed firewall, intrusion detection, virtual private network, vulnerability assessment, and anti-viral services. MSSPs leverage high-availability security operation centers (either their own or from other data center providers) to provide 24/7 services aimed at reducing the number of operational security personnel an organization needs to hire, train, and retain in order to maintain an acceptable security posture (Gartner, 2022).

In order to get the best possible answers and investigate "best practices", it was important for us that we learnt from experts working in leading organizations within the field of cybersecurity. Prior to this research, we had already agreed to collaborate with one leading MSSP based in Norway. The agreement was that during our research we would be allowed to interview candidates from this organization, and we were given a contact person that put us in touch with the right subjects based on our needs and their role in the organization. To avoid bias, we contacted several other organizations in the initial phase of the research which left us with one additional organization in the same category and scale willing to contribute to our data collection. In the table (3.2) below, the two investigated organizations are described.

	MSSP1	**MSSP2**
Description	Large multinational and leading IT consultancy company	Large multinational and leading IT consultancy company
Organizational turnover	Forty billion NOK (4.4 billion USD)	Forty-two billion NOK (4.5 billion USD)
Employees	Operates in 7 countries and employs more than 7,500 personnel	Operates in nearly 30 countries and employs 47,000 personnel
Business	Offers a full range of hardware and sofware from the world's top technology companies and help customers solve problems and get maximum productivity from their IT investments	Helps large private companies and public enterprises to take digital leadership, and is committed to creating value for customers and society with the mission of guiding their customers, partners and employees towards bold choices by leveraging digital technology to build a positive future for all
Selection motivation	We selected these firms as they: (1) have an in-house, state of the art SOC and permanent 24/7 IR function (both internal and as-a-service) that is mature and - amongst few, approved by an unnamed (sensitive) governing function, and (2) have evolved 'best practice' IR from experiences of highly sophisticated cyber-attacks.	

Table 3.2: Organizational profile of the two investigated organizations

When choosing informants within these organizations, it was important that they qualified to provide information and knowledge (Yin, 2014) that best suits our case. In order to provide a rich and broad picture of the phenomenon in the empirical findings, different roles of relevance within the organizations were interviewed. We made an inquiry to our contacts in *MSSP1* and *MSSP2* and shared our interest in interviewing; both junior and senior analysts working on their SIEM platform handling daily events, the CISO or other C-suite employees of relevance, a cyber-operations leader, a SOC leader, a cybersecurity strategy leader, and an employee working with cyber threat intelligence. This resulted in a total of 11 interviews, all of which provided valuable information to our research. We were determined from the beginning to ensure anonymity of our respondents and their employer, so that they could answer honestly without fear of repercussions. Figure 3.3 displays the role and years of employment of our respondents, where there is a wide range of experience and areas of responsibility amongst them, giving the answers from the interviews different perspectives. To avoid "elite-bias", which can occur if one bases the selection only on top management such as directors, board chairmen, etc. we included a variety of subjects in the sample at various organizational levels (Myers and Newman, 2007).

Pseudonym	**Role**	**Years in role**
CISO	Chief Information Security Officer	5 years
Manager_SOC	(SOC) Project Manager	0.3 years
Lead_IRT	Leader of Incident Response Team	7 years
TeamLead_SOC	Leader of analytics-team within SOC	2 years
L1Analyst_SOC	Tier 1 SOC analyst	1 year
Sec_Consult	Senior Security/Technical Consultant	1 year
Product_Manager	Manager of SOC services	15 years
Lead_Onboarding	Director Onboarding	1 year
CSO	Chief Security Officer	8 years
Lead_SOC	Professional Leader of SOC	3 years

Table 3.3: Subject selection

3.4 Data collection

Qualitative data includes all non-numeric data such as images, words and sounds found in interviews, researchers diaries and company documents to mention some. It is the main type of data generated in qualitative studies (Oates, 2006). In procuring knowledge information to be able to answer our research questions, to collect data, we made a choice of doing semi-structured interviews.

With a qualitative approach, interviews are designed to elicit detailed information, making it especially useful when a researcher's aim is to study social processes or the "how" of various phenomena (DeCarlo, 2021). When interviewing well-established large scale organizations dealing with cybersecurity on a daily basis there is a certain expectation that they have processes in place to maintain good SA within the context of cybersecurity. The expected outcome of the analysis is to develop an understanding on which elements and conditional functions are necessary to perform effective security operations in a busy environment and how to achieve holistic SA in that context.

An interview is a particular kind of conversation between people, and it has a set of assumptions that do not apply to "normal" conversations. We rely on interviews because it helps us better understand and explore research subjects' behaviour, opinions, phenomenon and experiences as our purpose for undertaking the interview is to gain information from the interviewee. The discussion does not occur by chance, but has been planned in some way by the researcher. They usually have an agenda—a particular set of issues they want to find out about—so the discussion of topics does not occur arbitrarily or randomly, with both sides free to choose the topics at will. Instead, the researcher will steer the discussion into their topics of interest (Oates, 2006).

The development of how we wanted to structure our interviews began with the reviewing of existing literature as described in the previous chapter. The literature review was important to be able to ensure greater reliability and validity of the questions that were to be asked. By understanding the findings of previous research, it was easier to tailor the questions in a way that would give value to the research.

3.4.1 Interview methodology

In qualitative research, multiple examined models represent semi-structured interviews (SSI) as indispensable tools for uncovering knowledge through interaction, conversations, and subjects from various life experiences. Semi-structured interviews are practical for undertaking in-depth conversations. Usually, the researcher can critically examine the conversations and first superficial responses to arrive at multilayered conclusions (Kakilla, 2021). For this specific study, SSI's were used as we wanted to develop certain questions to help us better comprehend our understanding of the topic and confirm or disprove specific aspects of our research problem. A SSI, in contrast to a structured interview, can delve into unanticipated concerns or topics. This approach helped us to discover more about the interviewee's own opinions and experiences, as well as how they perceived daily tasks. We experienced that the method allowed respondents to speak freely, and that we subsequently could ask for more precise details were we felt it was needed.

We wanted to ensure that the process of developing an interview guide was performed correctly and chose to follow a review paper: "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide" by Kallio et al. on how to make an interview guide using semi-structured interviews.

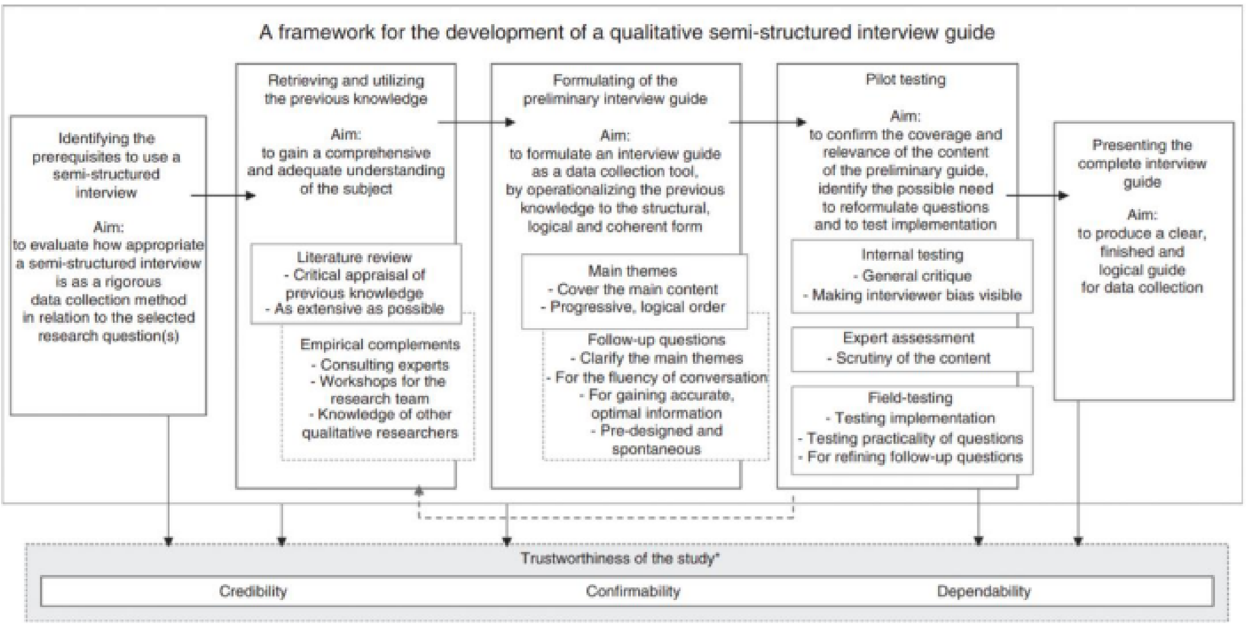

A framework for the development of a qualitative semi-structured interview guide
Identifying the prerequisites to use a semi-structured interview
Aim: to evaluate how appropriate a semi-structured interview is as a rigorous data collection method in relation to the selected research question(s)
Retrieving and utilizing the previous knowledge
Aim: to gain a comprehensive and adequate understanding of the subject
Literature review - Critical appraisal of previous knowledge - As extensive as possible
Empirical complements - Consulting experts - Workshops for the research team - Knowledge of other qualitative researchers
Formulating of the preliminary interview guide
Aim: to formulate an interview guide as a data collection tool, by operationalizing the previous knowledge to the structural, logical and coherent form
Main themes - Cover the main content - Progressive, logical order
Follow-up questions - Clarify the main themes - For the fluency of conversation - For gaining accurate, optimal information - Pre-designed and spontaneous
Pilot testing
Aim: to confirm the coverage and relevance of the content of the preliminary guide, identify the possible need to reformulate questions and to test implementation
Internal testing - General critique - Making interviewer bias visible
Expert assessment - Scrutiny of the content
Field-testing - Testing implementation - Testing practicality of questions - For refining follow-up questions
Presenting the complete interview guide
Aim: to produce a clear, finished and logical guide for data collection
Trustworthiness of the study*
Credibility
Confirmability
Dependability

Figure 3.2: A framework for the development of a qualitative semi-structured interview guide (Kallio et al.)

The idea behind following a framework represented in Figure 3.2 was to ensure that our interview questions are timely and relevant to the research questions, as every stage of the framework was met before we conducted the interviews. First we had to identify the prerequisites to use a semi-structured interviews in relation to our selected research questions as previously discussed. We conducted the literature review to gain a comprehensive and adequate understanding of the subject, and with this knowledge we formulated the preliminary interview guide. Following that, we ran a pilot test with the first draft of the interview guide to see if any questions needed to be reformulated in order to get the most out of the responses. We were now ready to conduct the interviews with our newly obtained information and the complete and final version of the interview guide B.

As we concluded that SSI's would be best suited for our study, we were aware of both the advantages and disadvantages following this method. Compared to other methods, SSI is very time consuming and intensive, meaning that we had to come well prepared before the interview. As well as being prepared, it is important to follow the respondents' answers along with being flexible to keep the interview adaptable. Before conducting the interviews, the participants were notified that the interview would be recorded as we wanted to go through the recordings afterwards to sort out all the details. We informed the respondents about all the formalities including anonymization of their statements and their rights to refrain from answering questions that they felt were too sensitive (See Appendix C: Consent Form). This agreement, which was included in the NSD application, explains how the information acquired in the interviews is processed and presented in this thesis. The goal was to have no correlation between the data collected and their company, so that no information could be linked to the companies. This was vital not just for the NSD application, but also for assuring the participants that the information would not be used against them in any way.

3.5 Limitations of interviews

Despite the many upsides and possibilities, there are potential difficulties, problems and pitfalls conducting qualitative interviews that can affect the outcome. In: *"The qualitative interview in IS research: Examining the craft"* Myers and Newman (2007) has compiled a list that summarizes the most common concerns about doing qualitative interviews:

- *Artificiality of the interview* - The qualitative interview entails questioning someone who is a complete stranger; it involves asking participants to give or to construct opinions under time constraints.

- *Lack of trust* - As the interviewer is a complete stranger, the interviewee is likely to have reservations about how much the interviewer may be trusted. This means that the interviewee has the option of withholding information that he or she deems "sensitive". If this is potentially essential data for the study, the data gathering remains incomplete.

- *Lack of time* - Due to a shortage of time for the interview, data collection may be incomplete. However, it can also lead to the opposite problem, in which interviewees form beliefs under time constraints (when these opinions were never really held strongly to start with). In this case more data is acquired but the data gathered are not entirely reliable.

- *Elite bias* - A researcher may only interview a few high-ranking people (key informants) and thus miss out on gaining an understanding of the broader situation. In other words, interviewing the "stars" in a company might add bias into qualitative research. Information from articulate, well-informed, usually high-status informants is overrepresented, while data from intractable, less articulate, lower-status informants is underrepresented.

- *Constructing knowledge* - Interviewers may believe that they are simply absorbing data or information and are unaware that they are actively generating knowledge. This can happen when an interviewee responds to a question they've never thought about before and reflects on it, while the interviewer takes that contemplation and turns it into something logical and consistent, but not what the interviewee reflected on.

- *Ambiguity of language* - Words might be ambiguous, and what the interviewer asks may not be what the interviewee hears, and vice versa, resulting in miscommunication between the interviewer and the interviewee.

The qualitative interview is a negotiated accomplishment shaped by the interview's social and cultural context. When used to its full potential, the qualitative interview is an extremely effective data collection tool. However, Myers and Newman (2007) believe that researchers should be more mindful of the potential problems and pitfalls associated with its use. The qualitative interview is a powerful instrument, but those using it should be aware of its strengths and weaknesses.

The limitations listed above were examined, discussed with the supervisors and taken into consideration before we started the interviewing process. An interview guide and consent form were developed and given to each subject to help build trust between the interviewer and the interviewee. The guide and consent form informed the interviewees about how the data they provided would be handled, stored and erased. Furthermore, whatever they said remained anonymous, and cannot be tracked back to them.

3.6 Data analysis

The analysis is based on the interviews, where we chose to make recordings rather than take notes during the interviews so that we can give it our complete attention. To analyze the interview contents, we went through the recordings of the interviews and transcribed them. The transcribed documents were subsequently analyzed and coded in NVivo, a software to aid qualitative research. By coding the transcriptions we derived answers to common questions from the different participants into categorized themes, which were beneficial to us when comparing and presenting our findings. After reading and developing an understanding of how it could be categorized, we identified specific segments related to the questions to label and categorize confirming or contradicting answers. The interviews were broken down into five sections, each of which was labeled to contain questions on the same subject. The questions vary from general questions about the candidate and their business in Part 1 to cybersecurity-related questions in Part 3 to a framework presentation in Part 5 where we wanted input on whether the framework accurately represented how incident management works in practice. Before presenting anything we had to translate the findings as the interviews were held in Norwegian, and we did it with utmost caution to prevent any translation-bias or misunderstandings. The findings section summarizes the answers, which are then contrasted to existing theories from the literature review in the discussion chapter. Appendix B contains the interview guide that was utilized during the 11 interviews.

3.7 Ethical considerations

When interviewing people, and people part of an organization whose operations surround security matters and security matters for customers, confidentiality has to be considered. While our investigations do not gather much sensitive data, there are some. Names, organization roles, responsibilities, processes and contact information that must be safeguarded. For this purpose, all interview material of recordings and transcripts are stored exclusively on encrypted and safe cloud storage provided by the University of Agder. The interview subjects have the right to revoke their consent, and have the right to gain insight on any stored material provided by them.

To collect and store information through our interviews it was necessary to submit a NSD application. The Norwegian Center for Research Data (NSD) is in charge of handling all research projects and maintaining a research data archive. According to NSD's website, they provide researchers with data handling assistance as well as a broad range of data and support services in order to improve the options for empirical research (NSD, 2022). Researchers are legally permitted to preserve and document their data once the NSD has approved their application. We were cautious to acquire NSD's agreement before storing or documenting any data in this research.

Chapter 4

Results

Following an inductive exploratory approach with elements from the interpretive tradition of qualitative research we have constructed a theory-informed narrative using a theoretical lens that resulted in the formulation of a conceptual framework.

4.1 The conceptual framework

By drawing on related literature and through sense-making of the theoretical lens, we have developed a conceptual framework depicting how enterprise security operations work and are operationalized to reflect our understanding of how SA is constructed through the different organizational levels: operational, tactical and strategic. The following framework (Figure 4.1 below) uses the logic of Endsley (1995)'s '*Situation Awareness' process model for human cognition* (see Figure 2.10) and takes inspiration from Ahmad et al. (2021)'s case study, combining their process model of *Situation Awareness in Cybersecurity IR* (see Figure 2.11) with their case unit "*FinanceCentral's*" information flow and communication pathways (see Figure 2.13)

The framework is modeled as a two-dimensional artifact. Cybersecurity stakeholders (L1 & L2, L3 and the SLT) are modeled across the vertical dimension representative to each of their organizational levels. The horizontal dimension models 'Situation Awareness' as of Endsley (1995)'s process model for human cognition that is framed from an information-processing perspective. The "background colors" blue, green and yellow represent perception, comprehension and projection respectively through the different organizational levels. The framework features three kinds of dynamic behavior. The first is information processing behavior (data-driven vs goal-driven), the second is task behavior (escalation vs investigation) and the third is communication behavior (information flow and communication pathways) (Ahmad et al., 2021).

Information processing behavior is modeled using the blue arrows in Figure 4.1 that allow progression through the 3 states of SA knowledge. Based on Ahmad et al. (2021)'s process model, the rightward pointing blue arrows reflect that organizations can acquire increasingly higher levels of SA from data-driven processes (moving from perception to comprehension to projection). The leftward pointing blue arrows reflect that goal-driven processing such as attention-focusing existing mental models can improve lower levels of SA (moving from projection to comprehension to perception).

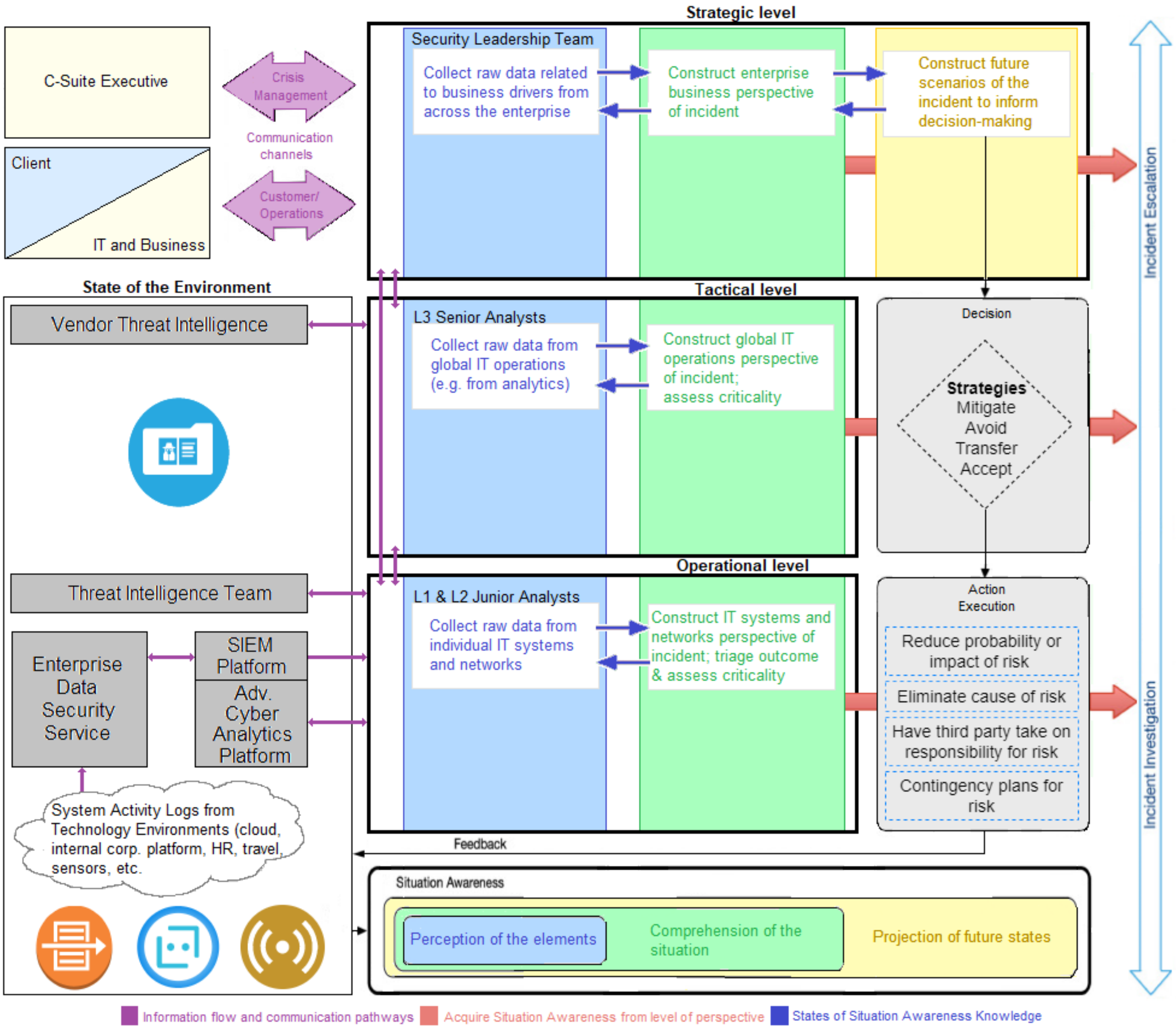

Strategic level
C-Suite Executive
Crisis Management
Communication channels
Customer/ Operations
Client
IT and Business
Security Leadership Team
Collect raw data related to business drivers from across the enterprise
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Incident Escalation
State of the Environment
Vendor Threat Intelligence
Tactical level
L3 Senior Analysts
Collect raw data from global IT operations (e.g. from analytics)
Construct global IT operations perspective of incident; assess criticality
Decision
Strategies
Mitigate
Avoid
Transfer
Accept
Operational level
Threat Intelligence Team
L1 & L2 Junior Analysts
Collect raw data from individual IT systems and networks
Construct IT systems and networks perspective of incident; triage outcome & assess criticality
Action Execution
Enterprise Data Security Service
SIEM Platform
Adv. Cyber Analytics Platform
Reduce probability or impact of risk
Eliminate cause of risk
Have third party take on responsibility for risk
Contingency plans for risk
Incident Investigation
System Activity Logs from Technology Environments (cloud, internal corp. platform, HR, travel, sensors, etc.
Feedback
Situation Awareness
Perception of the elements
Comprehension of the situation
Projection of future states
■ Information flow and communication pathways ■ Acquire Situation Awareness from level of perspective ■ States of Situation Awareness Knowledge

Figure 4.1: A conceptual framework of SA in SOC IR

Task behavior is modeled using the light blue outlined arrow on the right. Also based on Ahmad et al. (2021)'s process model, the upward pointing dimension represents situations where priority incidents are escalated from the operational level to the tactical level and ultimately to the strategic level stakeholders. The downward pointing dimension represents situations where the SLT or higher level SOC analysts require internal incident context to be developed by lower level analysts having been informed about a potential incident by stakeholders *not necessarily inside the SOC* (hence, lower level analysts have not already processed the information).

Communication behavior is modeled using purple arrows. Based on Ahmad et al. (2021)'s case unit, the large arrows in the top left corner illustrates crisis communication channels to the organization's C-suite executive and business management domains that *can be brought in as needed to provide additional context that assists with sense-making but also for delegation of tasks* (Ahmad et al., 2021). The smaller purple arrows illustrate how different technologies and stakeholders propagate information and communicate to and from each other. The bottom left module, based on Endsley (1995)'s *process model of 'Situation Awareness'*, the "State of the Environment" illustrates the sources of data-collection reflecting the operational environment to the SOC. In a socio-technical system, both the technological and human entities perform this function. Thus, the Enterprise Data Security Service (in the "state of the environment") collects system activity logs from the technology environments feeding raw data into the SIEM platform which promptly alert SOC analysts about suspicious behavior. Meanwhile, the dedicated threat intelligence team collects intelligence from a network of insiders among relevant institutions including sector CERTs, private collaborators, public agencies and law enforcement to provide actionable CTI to relevant stakeholders at the operational level. The vendor of threat intelligence similarly provides tactical intelligence to the tactical level stakeholders hypothesizing about threat activity impacting the organization and validating that against threat observations. (Ahmad et al., 2021).

The contributions of the stakeholders in each organizational level to *Situation Awareness* are represented by the red arrows. The L1 & L2 SOC analysts with a narrower (less experienced) frame of reference construct IT systems and network perspective, the L3 SOC analysts with a broader (more experienced) frame of reference construct global IT operations perspective and the SLT with an enclosing frame of reference (business-centered) construct enterprise business perspective of incidents. The states of SA collectively lead to the making of a decision and subsequently, by the impact of the decision, the interaction with the real-world environment (feedback) results in further modification of the operator's mental models which again directs further actions (Ahmad et al., 2021). Thus, when an alert is triggered on the SIEM, SOC personnel at the operational level triage whether it was triggered inadvertently or if the event indicate a strong likelihood of malicious activity. If the alert classifies malicious activity, it is escalated to a team on the tactical level that coordinates incident response (IR) and forensic activities with the owners of the involved IT assets. In rare cases of major incidents, the team must also coordinate with internal resources; IT and business domains and C-suite executives (legal and marketing) Bhatt et al. (2014).
Following the research design, we have constructed a theory-informed narrative using a theoretical lens that resulted in the formulation of a conceptual framework. This framework represents our interpretation of theory which models how security operations are operationalized to construct situational awareness and perform enterprise detection and response. By conducting interviews with cybersecurity specialists who knows best how it works, we test our understanding of theory and ultimately validate our conceptual framework through the practitioners feedback.

4.2 Empirical findings

During the analysis of the interviews we initially categorized the findings following the themes of the interview questions. But considering the exploratory nature of this study, we soon realized that we wanted to connect the findings of the interviews to the conceptual framework, in order to better construct a context which allowed for comparison and discussion with the theoretical lens in the subsequent chapter (discussion). Thus, the structuring of the empirical findings follows the dynamics of the theory-informed framework in order to create this context. In the following subsections we present our findings before discussing them in the next chapter.

4.2.1 Data collection of the environment

The inquired organizations (*MSSP1* and *MSSP2*) data collection of the environment is derived from multiple sources of information collection. The main channels are system activity logs from internal corporate networks (processes, files, network connections, authentication patterns and email activity etc.), cloud environments (cloud app usage and event logs), and customer's own systems. The evidence to support these findings are confidential, as *Lead_SOC* presented us with a model of sensitive nature of which we could not re-produce.

From the technology environments, the syslogs are channeled into collectors and then subsequently into the SIEM platform which correlate and accumulate the data. To produce security alerts and alarms, the SIEM performs real-time data analysis using a combination of vendor-issued standard detection rules and custom detection rules engineered by SOC analysts. *Product_ Manager* describes this:

> *"Depending on the customer, the [SIEM] tools we use for operating and analyzing data are QRadar and Sentinel. When QRadar is being used, we place it in our own data center, set it up according to our standard and procedures, and then we place an event collector function that is set up on a local server at the customer's which is then connected to their various sources, networks and environments. This goes for both on-prem and cloud solutions where we connect the event collector with a "site-to-site" tunnel that ensures data is gathered in a structured way."*

As he continues to talk about cloud environments, he describes how Sentinel is configured, describing how customers with primarily cloud environments integrate cloud collectors which directly channel logs to their SIEM.

> *"...as for Sentinel, it is normally used with customers having their systems in cloud environments as it is seamlessly integrated with e.g. Azure. The SIEM is set up in the customer's tenant in Azure and directly connected to the endpoints, sensors, logs and environments that are located in the cloud systems. For customers who do not have all their systems in the cloud, there must be a set of communication mechanisms manually set up to achieve this."*

MSSP1 and *MSSP2* are both IT and cybersecurity consultancies that offer security operations and incident response as a service in addition to protecting their own perimeter. Therefore, following up with customers on security is a big part of their everyday tasks. When it comes to data collection *Lead_ Onboarding* emphasizes that the client is involved in determining what to monitor:

> *"It is based on what the customer has chosen to collect, but the typical endpoints will be the server and network environment, such as switches, firewalls, and possibly other systems over which they have a specific need for control. The customer is involved in the decision-making process, but there will always be cooperation. Best practices are what we bring as professionals, but the customer may have special systems and peculiarities that we must map, or that the customer is aware of and that contribute to the overall threat picture that must be monitored and controlled."*

Both organizations employ a 'service desk' alongside the SIEM that handles phone calls, alarms and tickets from customers who experience irregularities on their systems. As we just explained, both organizations offer SOC and IR as a service, and thus, customers must have the opportunity to reach out, should something not be picked up through the cloud and on-prem sensors. Through conversation with several interviewees (*CSO, Lead_ SOC, L1_ Analyst*) we understood the service desk functions much like the dashboard of SIEM systems. The analysts monitor a dashboard reflecting the service desk which visualize "customer input" i.e., tickets explaining system irregularities.

As we move along from the technology environment to the human operators reflecting the state of the environment, *Lead_ SOC* points out that there are several good tools from which threat intelligence teams can obtain information from, and states that:

> *"Feedly, among other tools, is widely used by cybersecurity professionals to stay up to date on the latest security news and research insights about critical threats (threat actor groups, vulnerabilities, data breaches and malware, etc.). MISP, an*

> *open source software solution for acquiring, storing, distributing, and sharing cyber security indicators and TTP's (tactics, techniques and procedures), is another excellent and extensively used application."*

Using feedly, the CTI team stays current with the operational environment and propagates actionable intelligence to relevant parties across the SOC team as they see necessary.
As of now, neither *MSSP1* nor *MSSP2* subscribe to third-party vendors that sell cyber threat intelligence, and it is questioned whether it is worth the investment. *Lead_IRT* on investing in threat intelligence:

> *"We do not currently purchase ready-made threat intelligence, and this has been a topic of discussion for some years. We really want to buy access to Recorded Future, for example, but it is really expensive. So, in order to persuade management, we'll need a strong business case that answers the question; "What does it give us beyond what we can accomplish reasonably well today?". and that is fair, as we were working on a ransomware case last year, and I happened to be sitting with Recorded Future London at the time. We fed a couple of the IOCs we got from our sources, and they didn't detect anything different than what we found in open sources. The benefit of employing Recorded Future though, is that they collect for us rather than us having to work in a variety of disciplines manually."*

The inquired organizations both collect information from the environment through on-prem physical sensors and through cloud collectors in the customers technical environments. They both use the SIEM tool Microsoft Sentinel primarily for cloud environments and use mostly IBM's Qradar to monitor customer systems in physical environments. We had the impression that both organizations were phasing out Qradar, using Sentinel more and more, on account of cloud popularity among customers. Both organizations deny the use of intermediary systems between the syslog collection and the SIEM tools. The customers are involved in choosing which data to monitor but are advised by professionals to make a decision. Both organizations employ service desks to reflect the state of the customer environments through arbitrary use of tickets and calling systems if the SIEM haven't already picked it up. To collect threat intelligence data and stay up to date with the operational environment, the organizations use tools like Feedly but they do not subscribe to ready-made CTI from specialist vendors.

4.2.2 Threat intelligence team

Both of our studied organizations receives threat intelligence that helps them identifying threats. A key source for *MSSP2* is their dedicated team that collects intelligence from a number of sources such as; national and international CERT's, social media platforms, specialist vendors, and reports from national authorities. Another key source are referrals from the first-line (*L0*) service desk and employees reporting phishing attempts or other suspicious activities. This threat intelligence function is described by *Lead_SOC*:

> *"As part of our SOC, we have a small team of analysts working with cyber threat intelligence. In general, their job entails consuming what is going on in the world and transforming it into something actionable internally. We are in some other forums as well, and we experience that there is a lot of good intelligence, not only information, but also ready-made intelligence in open sources eventually. Today's situation is something completely different than just 5 to 10 years ago, where things very quickly became both TLP:AMBER and TLP:RED, just because it's about security. Now you will find just as good actionable information from government entities with liberal TLP and commercial sources like vendors producing threat reports have a lot of good, actionable information that can be used. This makes*

> *working with threat intelligence easier today because you don't have to be in all of the closed environments."*

There are several ways one could accumulate threat intelligence, and *MSSP1* has another approach and division of roles as they do not operate with a dedicated team collecting and working with threat intelligence. It is more up to each individual to stay informed about the threat landscape and engage in threat hunting. On the situation of threat intelligence *Lead_IRT* states:

> *"Basically, it is a daily task to follow a long list of feeds. There are several aspects - one is attacks that occur and identifying new threat actors and their TTPs(tactics, techniques and procedures), what new elements may appear, such as vulnerabilities that we must inform customers about in order to be proactive. Another is status meetings that we have every Monday morning where one of the main points are threat intelligence, and the objective of the meeting is to update everyone (in the team) on the current situation. We currently have very manual processes in place, but there are daily tasks to obtain and document information that is shared across different teams. This data is then structured and "translated" into understandable content in the form of reports, which are then partially or entirely handed over to the customer in relation to the situation."*

A large part of reducing cybersecurity risk requires information sharing and collaboration among a diverse set of actors using a variety of models, methods, and mechanisms. Wagner et al. (2019) (2.5.1) explains that sharing of CTI is an effective way of enhancing the situation awareness of an organization and its stakeholders. *MSSP1* and *MSSP2* are generally open to share threat information without being able to disclose specific collaborations with consulting firms in the same industry. In Norway, with the sectoral response environments (financeCERT, powerCERT, healthCERT etc.), there is some debate about whether an itCERT will become more necessary, as the IT-sector evolves. *Lead_SOC* describes the situation:

> *"I'm not going to opine on whether it should be an itCERT or not; all I'm saying is that it doesn't exist, and as far as I know there is no "threat intelligence circle" in Norwegian IT industry. We live well with one-to-one sharing across the enterprises that matter to us, and I know that many of my colleagues, like myself, have personal networks with whom they share information. That said, First is worth mentioning, which is a global forum for incident response teams. Although it is a global community, there are rather strong local communities "under the umbrella" in several countries, and Norway is likely one of the more active communities in First."*

Empirical research opposes theory and reveals that leading cybersecurity specialists do not use STIX to the extent described in the theory chapter by Sauerwein et al. (2017) 2.5.1. In fact, it turns out that MISP is the favored method for communicating cyber threat intelligence across stakeholders, and *Sec_ Consult* explains that:

> *"In our collaborations with various CERTs, they use a platform called MISP rather than STIX. This is because STIX removes too much data, leaving you with insufficient details. With STIX/TAXII, you are locked into the framework that has been established, and you do not have many options, whereas with MISP, you have several options and more freedom in terms of wording. If desired, MISP also has the ability to transfer images."*

The cyber threat intelligence team communicates and share information on multiple levels (operational, tactical and strategic level). The team collects and disseminates operational-level alerts and raw data to L1 and L2 SOC analysts, tactical level alerts to L3 SOC analysts, and strategic-level alerts to the Major Incident Team. *TeamLead_ SOC* shares an example of how their CTI team operate:

> *"I believe the CTI team is at the tactical level, and that they provide operational level analysts (L1 & L2) with actionable intelligence, as the CTI analysts never acts on their own information. The CTI analysts extract the critical information and "send it down" to the operational level analysts, who, for example, create a detection rule for these IOCs.*

4.2.3 The operational level: Handling low-severity incidents

> *"So, primarily at the operational level, there is always someone on duty 24/7, awake and working in front of the SIEM to perceive if something happens; and, if an event occurs, it is captured by either the SIEM through an alarm or by customer ticketing at the service desk - or by both."* Lead_Onboarding

Perceiving the environment from multiple sources of information is a key detail for Level 1 and Level 2 SOC analysts. To construct the IT systems and network perspective, Level 1 analysts are full-time responsible for the triage of all initial security alerts and the handling of low-severity incidents as described by Vielberth et al. (2020) (2.3.2). In the triage process, less experienced L1 analysts especially lean on playbooks (guidelines) and use cases (set of rules) to piece together and make sense of an incident, as *L1_ Analyst* explains:

> *"So, graduates or more recently employed SOC analysts, we lean very much on playbooks written by seniors. That is basically part of my typical daily tasks; to sit there and monitor alarms coming in to the system - we receive alerts both on the SIEM and on the service desk, and then typically we go in an check the alarm, and if it requires further investigation, we have more detailed tools like playbooks and automated use cases, where we dive even deeper in to it. So this is basically what we do, we sit and work in the SIEM most of the time handling the security events and false positives we receive."*

Level 2 SOC analysts manage incidents much in the same way, though they are more experienced and require less guidance by playbooks and use cases. Thus, they are more efficient and also they find it easier to develop a picture of what is going on with a situation as described by Vielberth et al. (2020) (2.3.2). Beside handling incidents, they also provide assistance for Level 1 analysts if an alert or ticket is too complex for them to handle (e.g., if it is unclear if an incident-trigger is a false positive or not) or if it might be something more serious that needs attention from someone with the capability to distinguish "what is going on".

> *"The level 1 analyst typically react to most of the incoming alarms; They start perceiving what has happened, and gets a quick overview - and if he or she either can't manage or don't know how to manage an incident, because it may be complicated or is more serious than they are comfortable with, the case is immediately bumped to level 2. The level 2 then delves into it and performs the actual analysis; scrambling through the system to construct a better picture of what is going on."* Sec_Consult

Developing use cases and playbooks for the lower level analysts to use is the tactical level (L3) analysts with a broader perspective and even more experience. Where the L2 analysts typically are team leaders on the operational level, L3 analysts *have lead* and oversee the operational domain, making sure they have the resources and the tools necessary to tackle everyday:

> *"I, who am lead analyst in our team, on level 3; if i can help make everyday work easier (for lower level analysts) and build detection - I would much rather do that than [just] being an escalation point from level 2. What I do is I enable level 2 analysts to handle more things themselves, and that is the way we want to work."*
> Lead_SOC

Lead_SOC presents us with this model (Figure 4.2, (which we have 'anonymized' and simplified)), when he explains the process from perception to comprehension at the operational level to potentially making an escalated tactical decision to either inform or act upon a registered threat. This is one example of many tactical instruments developed and deployed by level 3 analysts to ease and specify processes for the SOC and lower level analysts.

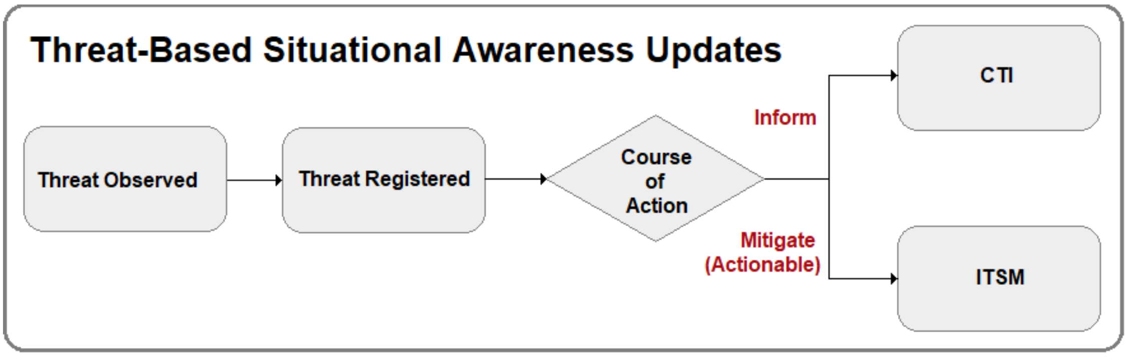


Figure 4.2: Threat-Based Situational Awareness Updates decision tree

> *"So, this phase right here [points to Figure 4.2], this is really where you observe an incident and take it into your understanding of the situation. Where you have called it "Perception" and "Comprehension", I have called it "Threat observed" and "Threat registered". And this can really be anything from "right now, Log4J is vulnerable" to "wops, it seems that a firewall at one of our customers have been misconfigured, so the attack surface is now much larger". So, in these cases we have SOPs (Standard Operating Procedures) and routines to take care of this. And so typically, when an alarm goes off at one of our customers, it goes into the SIEM or through ticketing, and having registered a threat we have that split, meaning "Is this something we should just inform about?" or "Is this something that is actually actionable?". And if it is a concrete cybersecurity incident that has happened, we follow the ITSM (IT service management) path here and integrate with business operations at the customers location to start handling the incident"*
> Lead_SOC

Consequently, the *Lead_ Onboarding* explains how the use cases and playbooks work in practice, and how they eventually help in the escalation process when an actionable incident is registered:

> *"So, the use cases and playbooks work in such a way that when the SIEM catch something particular, for example if one has experienced a certain hacker incident earlier from a given IOC (indicator of compromise), you can have a use case that tracks every log-on attempt happening from that given address, and then you will have a playbook which for example says "for these cases; immediately escalate to SOC level 2 for analysis to see if it's something real, or if it is just another false-positive", and then if it is real: "OK, bang, escalate straight up to what we call IRT, because this is an attempted or ongoing breach. And that's when you have to respond. In such a case, the IRT take hold of it immediately and begin response, and you begin contacting customers to have a system shut down or taken down which is under attack. And it really goes very fast (from threat detected to IR)."*

4.2.4 Response to high-severity incidents

Low-severity incidents are fully managed on the operational level without the need for escalation. High severity incidents such as a confirmed compromise of one or more systems, are immediately escalated to the tactical level by operational level analysts.

> *"The tactical level is an escalation point for when something is too big, typically, for the operational forum. So if for example we have a discussion on if we're rolling out new endpoint agents in a larger part of the environment or, making some changes in a security zone [making changes to security architecture to mitigate a threat/risk] - at that point it is no longer the SOC that sit and speak with operations at the customers'. At that point it is important that it is those that control IT [technology] that have that same talk with those who maybe control the budgets on IT. And there, we're not only talking about the handling of incidents, but the handling of risk. So what we see as a threat here is like "these five vulnerabilities exist and are widespread" and may be a risk on the tactical level of which the customer have calculated ownership. So what we do is we build a good risk register and do that job, with a good management system etc., and all that governance-related business lie on the tactical level. And then we make the right priorities to put the directors in a position to make good long-term decisions for their business".* Lead_SOC

So at the tactical level, when something is too big for the operational forum, the *Lead_SOC* and L3 analysts coordinate and start pulling on resources that are more fit to handle a given situation. The analysts on the operational level are experts on analysis and can handle low-severity incidents but when we are talking about hands-on technical incidents, typically, this is when you call for the incident response team to handle the situation:

> *"On L3, that's when something happens. That's typically when the incident response team moves out, or the incident responders that is".* CSO

In rare cases of major incidents, the tactical team coordinates with the major incident team on strategic decision-making. The *CISO* showed us the different classifications for Major Incidents (MI) in *MSSP1* and explained that MI1 is the highest priority saying "*Datacenter Down (All/Everything)*". MI2 has two branches with different criticality, saying "*MI2(3) - 2 or more customers expected to be down for over 6 hours*" and "*MI2(4) - 1 large/important customer expected to be down for more than 6 hours*". The lowest MI priority is MI3: "*2 or more larger/important customer affected*". Reflecting on the classifications however, the *CISO* explains that:

> *"while the different criteria state the importance and grandeur of a client to decide for their priority, we don't really have a specific definition as to what is an important customer or not, but if someone says that a customer is important then we are on it."*

Moreover, the *CISO* informs that MI1 is more of an infrastructural case of incident and does not necessarily involve cybersecurity. In the case of a cyber attack it is typically within the MI2 category. The specified 6 hours does not either really mean that the attack lasts for 6 hours, but that it typically takes at least 6 hours to build it back up. For the purpose of perspective, the *CISO* informs that they have had and surpassed 20 customers with ransomware variants in the past year.

Depending on criteria and priority, if for example a large and important customer is expected to be down for more than 6 hours as a result of an incident, it triggers the rare formation of the Major Incident Team (MIT). In such an event, the *CISO* explains typical routine for the first responders to assess:

> *"In the event of a serious incident, the 1st line SOS/security team must assess the following: (1) Acquire information and evaluate incident on premises (2) Make decision on if we have a crisis situation based on the given criteria for premises (3) Alert responsible for crisis management of premises/incident (4) Alert responsible for crisis management in operations if necessary (5) Make sure of general information to affected parties on premises/incident".*

Thus, as the first line responders of the MIT have assessed and classified the incident, their responsibilities (which tend to be executed in parallel) is to open communication channels to all relevant stakeholders and direct the enterprise response. To execute these responsibilities the MIT initiates a formal 'IT Service Management process' referred to as ITSM which you may recall from Figure 4.2 (if an observed threat is deemed actionable, they initiate ITSM). Through ITSM they integrate with business operations at the customers location to start handling the incident with the customer. Consequently, a designated emergency manager "owns" the incident, and starts setting up a crisis team. The *CISO* explains:

> *"He creates a case in CSMS (Cyber Security Management System), defines who are crisis leader, who are information manager, and who are technical leader. From there, they set up MS Teams channels; one leadership channel for the crisis team itself and one channel for customer information. As the customer channel is established, they begin solving the crisis by gathering resources and looking at security measures. Every thirty minutes, to begin with, we also inform affected customers by SMS, including relevant internal staff. Typically leader-groups in MSSP1's operations unit gets an alert every thirty minutes as well."*

Hence, in the framework (Figure 4.1), the Business and IT domains module relates to the ITSM process and customer channel whilst the C-suite executive module relates to the CSMS process and leadership channel.

An important distinction between *MSSP1*, *MSSP2* and Ahmad et al. (2021)'s "*FinanceCentral*" is that the latter is a financial organization with responsibility for their own perimeter alone and not for others'. *MSSP1* and *MSSP2* however, are both IT and Managed security service providers who provide security operations and incident response as a service beside also defending their own perimeter. That makes certain distinctions as to e.g., the meaning of *the* environment. Thus, have in mind that interviewees speak more often than not about customers' situation as opposed to their own. Nevertheless, operations and processes as illustrated in the framework are equally applicable to an external environment with external IT and business domains and C-suite executives in the mix. This is represented by an asterisk in the framework (e.g., IT and Business Domains*) where applicable. Lead_SOC explains:

> *"If we have a concrete security incident that has happened (with a customer), we integrate with the operational processes that the customer has - because the point is, in very many cases, we are not only the ones who say that "we have seen an incident", we are also the IT department of the customer - handling the incident. So for our part it is not just an arrow out to the customer, it is: "OK. Now we sit with the customer and work" - to a large extent. But the 'customer' could well also be our own business operations."*

Hence, the business management domains can be brought in by the *Major Incident Team* as needed to provide additional context that assists with sense-making, but also for delegation of tasks, be it externally with the customer or in the case of an internal cyber incident. Depending on the impact and, in the case of a major incident *Lead_ Onboarding* explains and refers to the IT and business domains:

> *"We drum together all the people you need to meet this challenge; it can be anything from server people, network people, backup people, file and storage people,*

> *etc., and, of course the incident response team is involved. Everyone needed to tackle the situation are drummed together in war-rooms and task-forces to start correcting the error to eventually get the customers back on their feet allowing them to maintain operations as well as possible."*

Here, more often than not, communication is held through digital communication channels as referred to as "war-rooms" by *Lead_ Onboarding*, typically through MS Teams channels or similar. In parallel, while operations are under way, the *Major Incident Team* will engage with the CISO and senior executive through the crisis management *war-room* if not on premises.

> *"During incident management, the leaders are involved, yes. If the incident is big enough and decisions need to be made by those with the power to do so. And in the incident response team; they have people that can travel to the customer and be on-prem if need be.* Lead_Onboarding

Thus, meanwhile engaging in knowledge sharing about the incident and its changing context, the *Major Incident Team* will keep regular situation briefings and obtain sign-off on important decisions with C-suite Executives. The *CSO* explains some of the assignments he and the *CISO* do internally when an incident happens:

> *"If we have an incident, in strategic decision making I am the one who see the economics part.. I probably see it very differently than those who work in the first and second line here, but it is about making people aware in terms of risk and loss of money. I also make sure that we handle the incident correctly according to the media, and start a contingency plan in case someone contacts us in relation to if it's being done correctly and what we are going to do. And then I'm straight in to talk to communications directors and explain to people what to say. The CISO on the other hand addresses the legal aspects of the incident and makes sure that what we do and how we deal with the incident is within the law and within the law of information security"*

The *Major Incident Team* with the *CSO* will also present the C-suite executive with a risk and impact assessment of the incident to inform decision-making. When a customer is faced with a major incident, their leaders need to have the courage to make major decisions. There could be risk of reputational damage, disclosure of intellectual property, customer data and considerable monetary losses:

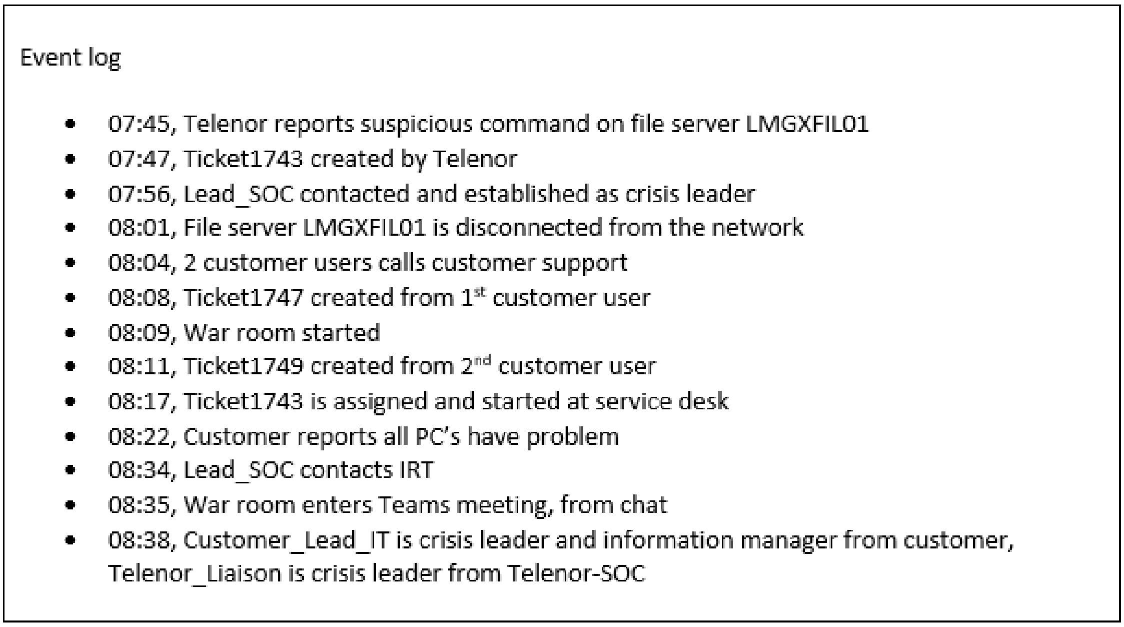
> *"When you begin conversing with management to make a decision, that is when we on the upper strategic level get on board; we know business management and at the same time we can illuminate... "If you don't do this - it will cost you this" right, like - "We know your business model and your customer base, and bad publicity can cost you this". For example, it could be the scenario that "If we don't do something right now, you could risk losing 4% of your total turnover, and that is when we start talking about real money."* CSO

4.2.5 The aftermath

Following the major incident team's calculated decision and subsequent action execution, it is critical to consider what to do after an incident has occurred. How you handle an event after it's over is just as important as how you handle it while it's happening as discussed by Cichonski et al. (2012) (2.3.3). It's critical to have systems in place after an event that ensure you assess the situation to determine whether; you did the right thing, was it completed in a timely manner, did you have the optimal mechanisms in place to solve it, and so on.

The event log (figure 4.3) is a recreation of a shared document from the *CISO*, which represents an invented scenario that is part of the employees' training to, among other things, increase situational awareness in the organization. Going through the incident and highlighting what processes have been done at what time can be helpful in understanding what may have gone wrong, and possibly figuring out which procedures need to be improved. The *CISO* expressed that:

> *"In this specific event we can see that IRT was contacted way too late, nearly an hour after the suspicious command were detected, and that is something we need to learn from. This is definitely something that would be added in the "lessons learned" report."*



Event log

- 07:45, Telenor reports suspicious command on file server LMGXFIL01
- 07:47, Ticket1743 created by Telenor
- 07:56, Lead_SOC contacted and established as crisis leader
- 08:01, File server LMGXFIL01 is disconnected from the network
- 08:04, 2 customer users calls customer support
- 08:08, Ticket1747 created from 1st customer user
- 08:09, War room started
- 08:11, Ticket1749 created from 2nd customer user
- 08:17, Ticket1743 is assigned and started at service desk
- 08:22, Customer reports all PC's have problem
- 08:34, Lead_SOC contacts IRT
- 08:35, War room enters Teams meeting, from chat
- 08:38, Customer_Lead_IT is crisis leader and information manager from customer, Telenor_Liaison is crisis leader from Telenor-SOC

Figure 4.3: Event log (recreation)

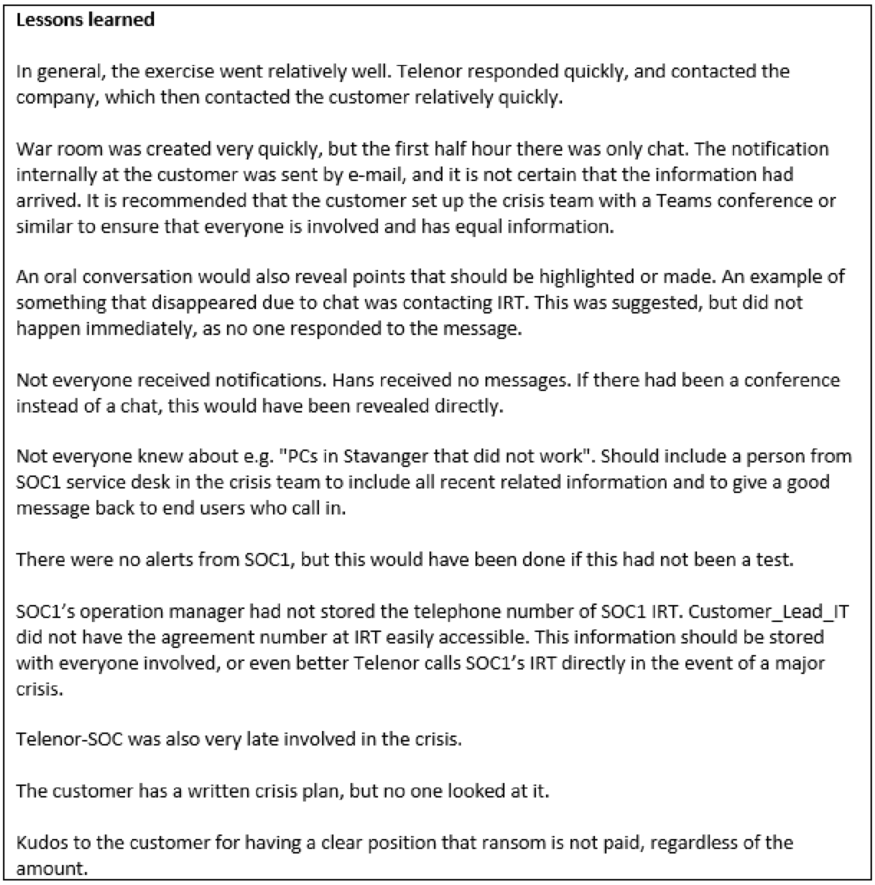
As the *CISO* continues to discuss the aftermath of an incident, he hands out another document (figure 4.4) detailing the lessons learned from the made-up scenario. The document contains all positive and negative findings from the event, and *CISO* points out that: *"MSSP1's operation manager had not stored the telephone number of MSSP1 IRT, and Customer_Lead_IT did not have the agreement number at IRT easily accessible"*, which could be reasons why IRT was contacted too late in this specific scenario.

However, "Lessons Learned" is utilized not only after incidents, but also during weekly debriefings:

> *"Once a week, we have a 'Lessons Learned' meeting where we debrief on everything that has happened, whether it is related to security or not. Typical scenarios include: were we quick enough to notify? Is there anything we could have done differently? Then we sit down and go over the whole list of thoughts to see if there is anything we can improve. It's possible that as a result of this, the architecture may change, or that we'll have to make certain GPO adjustments, such as registration modifications or group policy in Windows for example, that affect all customers"* CISO

MSSP1 and *MSSP2* have both integrated "Lessons Learned" into their procedures to better prepare for future events.

> *"Lessons learned is perhaps the most important step after everything has been packed together, and the incident is over. It is the matter of sitting down and talking through the incident; what actually happened, what could have been done differently.* TeamLead_SOC



Lessons learned

In general, the exercise went relatively well. Telenor responded quickly, and contacted the company, which then contacted the customer relatively quickly.

War room was created very quickly, but the first half hour there was only chat. The notification internally at the customer was sent by e-mail, and it is not certain that the information had arrived. It is recommended that the customer set up the crisis team with a Teams conference or similar to ensure that everyone is involved and has equal information.

An oral conversation would also reveal points that should be highlighted or made. An example of something that disappeared due to chat was contacting IRT. This was suggested, but did not happen immediately, as no one responded to the message.

Not everyone received notifications. Hans received no messages. If there had been a conference instead of a chat, this would have been revealed directly.

Not everyone knew about e.g. "PCs in Stavanger that did not work". Should include a person from SOC1 service desk in the crisis team to include all recent related information and to give a good message back to end users who call in.

There were no alerts from SOC1, but this would have been done if this had not been a test.

SOC1's operation manager had not stored the telephone number of SOC1 IRT. Customer_Lead_IT did not have the agreement number at IRT easily accessible. This information should be stored with everyone involved, or even better Telenor calls SOC1's IRT directly in the event of a major crisis.

Telenor-SOC was also very late involved in the crisis.

The customer has a written crisis plan, but no one looked at it.

Kudos to the customer for having a clear position that ransom is not paid, regardless of the amount.

Figure 4.4: Lessons learned (recreation)

You place yourself in a position where you can be exposed to the same type of incidents again if you do not learn from and work through the events that occur. *Lead_IRT* on the term "lessons learned":

> *"Unfortunately, we encounter a lot of people who work from "start to finish" during an event, then move on to the next one without necessarily refining processes or learning from past ones. If you want some feedback, I'd say that a form of quality assurance is good practice; that is like 'which assessments were done right?' and 'what was the choices we made?'"*

Reflecting on the decision and execution of the conceptual framework, *TeamLead_SOC* made the point that decision-makers must practice regularly in order to improve the effect of overall quality of their decisions:

> *"Do you really have it all figured out? - what one decision will lead to versus another? You don't know that until it happens, right? And that - is the awareness you should have when making a decision, but it is deficient because not enough people practice making that decision".*

4.2.6 Information sharing

Although "information sharing" is not currently part of the framework, it could potentially be included in an expanded framework as a result of further research. Findings of the literature review revealed that organizations are not generally interested in exchanging information with other organizations when they are confronted with a cybersecurity incident. Our impression from existing literature is that organizations are hesitant to share cybersecurity information with governments, partners, and competitors as described by de Fuentes et al. (2017) (2.5.1). Lack of trust in the sharing infrastructure, particularly if it is controlled by a possible competitor or adversary, and the manner in which sharing is carried out are among the reasons. That said, we got a slightly different impression after conducting the interviews, as it turned out that both organizations are willing and positive to share information as *Lead_ SOC* states:

> *"We are very open to sharing information - without naming specific partnerships, but we do have some, and they are typically one-on-one relationships."*

This is further supported by *CSO* as he explains:

> *"We collaborate closely with other organizations in the same industry, and these are companies that have been approved as incident handlers by the national security authority. We always act in the best interests of the customer, employ the same methodologies, and collaborate really well."*

It can be argued that this only applies at the "strategic level" and does not reflect how it will be resolved at the "operational level". Based on the feedback from *SEC_ Consult*, who works as a technical consultant on the operational level, it is to believe that information sharing of threat intelligence is not something he is involved in, as he gives a different perspective on the situation:

> *"I wish there were more collaboration with other organizations working in the same industry. Right now, management sees sharing information as giving a competitor a competitive advantage. We in the security profession have a different perspective on the situation, and we see far more benefits than drawbacks to such collaboration, even between competitors."*

The assumption that those who do not work at the strategic level are not involved in, or are unaware of, the sharing of threat intelligence with competing organizations was reinforced when *Product_ Manager* revealed that:

> *"I simply do not know if we are cooperating with our competitors, but I do not think so."*

4.3 Practitioners input

Through this research also in an early stage we collected the practitioners input to create and develop the initial conceptual framework (section 4.1). To further collect the practitioners input as a last step in our interviews that we conducted; we designed a scenario-based small exercise where we asked the interviewees to follow the conceptual framework described in section 4.1 and provide us with their reflection. Following this process, helped us systematically collect feedback from the practitioners and then further develop the individual components inside the framework. We intentionally put this step into our interviews to include it here and that is why we are presenting these results. The goal of our interviews was first to collect information and then to collect feedback and validation through the scenario.

The *Manager_ SOC* did not have many contributions to the many technical questions we posed during the interview. With a project manager background, her role is to manage the SOC team and the overall management processes "behind the scenes" more so than inside the SOC. When presented with the framework, she found the workings and processes it represents quite fitting to their working philosophy:

> *"We have something we call the "cyber defence loop", which kind of is the philosophy we work by, it reminds me very much of this. We gather all the data; the data becomes an overview of the threat picture; which becomes guidance for detection development; which is again used in monitoring; and consequently in incident handling; and then we learn from it, we call it lessons learned, and then it returns to the operational picture again like a loop. So it actually reminds me of that.* Manager_SOC

Lead_SOC offered a great deal of insight to our overall interview and gave extensive feedback on a lot of aspects. He as a leader of the SOC on the tactical level with both forensic and incident response capability presented a lot of high value findings for us. When presented with the proposed framework, he was amused as to how much he could relate:

> *"This is very cool. I recognize a lot - and it is, well, it is kind of amusing - because a lot of what I see here, we have in our own variants. This model - and a lot of what we're discussing today with the SOC is exactly just this."* Lead_SOC

The *Lead_IRT* also had a great deal of insight to our overall interview. He is the leader of *MSSP1*'s incident response team and has many years of experience behind him. When presented the framework, he especially reflected upon the feedback-aspect of the framework and expressed an increased taste for the emphasis on situation awareness on different levels:

> *"My immediate reaction is basically very positive. This was kind of cool to see. I find it pretty close to reality - the way i experience it. Of course it gets a bit theoretical in relation to practise but I really haven't worked much on the SOC in that respect, and I don't know exactly how they work, but - I really appreciate how you split it up in situation awareness on different levels, because that really is different things. And feedback, not to forget - that you have that in the loop".* Lead_IRT

Lead_Onboarding, our main point of contact through *MSSP1* has been with us since the beginning. He makes the point that you can't generalize everything, as some parts of our framework are different to their organization. Nevertheless, he states that it is correct in perspective of how SOC and incident response works and are operationalized, which in the end is our objective:

> *"Completely related to how we do it in MSSP1 it is not, but that doesn't mean that - in principle, this is completely correct. I do not see anything wrong with what you say here, at all. You have all the elements; we maybe call it something else; you maybe do things a little bit different, but that does not mean that others do not do it the way that you do - so in principle, I think this is pretty much spot on."* Lead_Onboarding

The *L1_Analyst* works at the operational level, handles tickets from the service desk and monitors the SIEM when he's not busy handling alerts and low-severity incidents. When presented with the framework, he found it quite level with how it works in reality. He was however the first to state that they did not formally utilize the distinctions "junior" and "senior" in their SOC, which is something we took to heart and changed in the framework. Moreover, he informed us about how seniors on the tactical level indeed were the ones to build the playbooks and use cases for the L1 & L2 analysts to use when an incident happens.

> *"Immediately I think a lot of this sounds very correct, and a lot of it correlates very well with how we want to work in the SOC. Though, while we kind of have both juniors and seniors in our SOC, seniors could well still work on the operational level - but on the other side, I do agree that seniors are the ones at the tactical level and upwards because they have more experience and have more overview of how things work. But all in all, i think you've pulled this together pretty good, on how things work".*

L1_ analyst also made one very interesting comment, which while it is hard to illustrate in such a generalized framework, is worth mentioning:

> *"Here at MSSP2, an L1 or L2 analyst for example, can have main responsibility for a specific customer, and if that customer have an incident, then that analyst may well be included in the upper levels (MIT). Because, meanwhile yes we may only have worked with cybersecurity or on the SOC for one or two years, but we have very specific data and information; and situation awareness for that specific customer. And thus, even a junior could be part of such a major incident team."*

That is an important point to make, and while the purple arrows in the framework may illustrate this by the information flow and communication pathways, it is worth describing in more detailed when reflecting on the major incident team.

Chapter 5

Discussion / Summary of findings

The objective of this study have been to examine how MSSPs implement security operations to i.a. construct situational awareness. By narrowing it down and looking into best practices as to how this is done within security operations centers (SOC) of large scale cybersecurity enterprises, the objective of this exploratory study have been to develop a generalized and holistic framework visualizing the workings of an operational SOC. Meanwhile, goals were to examine and understand situational awareness in cybersecurity incident management and identifying conditional elements, functions and best practices involved to support SOCs in achieving this.

Following an inductive exploratory approach with elements from the interpretive tradition of qualitative research, we have constructed a theory-informed narrative using a theoretical lens to produce an iterative understanding that resulted in the formulation of a conceptual framework. Our proposed framework was then validated through interviews to eventually produce an empirically validated, final framework. In this section we present our empirical framework and discuss the findings from the validation to answer our research questions.

5.1 A Dynamic Framework of Situational Awareness in Cybersecurity SOC-IR

As a result of comparing the conceptual framework (Figure 4.1 with empirical inquiry, we have developed an empirically validated framework modelling how SOC-IR works and are operationalized to understand how SA is constructed through the different organizational levels of 'best practice' MSSPs. The following validated framework (Figure 5.1) is an outcome of the literature review using the logic of Endsley (1995)'s *'Situation Awareness' process model for human cognition* (see Figure 2.10) and, drawing inspiration from Ahmad et al. (2021)'s case study, the framework combines their process model of *Situation Awareness in Cybersecurity IR* (see Figure 2.11) with their case unit *"FinanceCentral"*'s *Information flow and communication pathways* (see Figure 2.13). Finally, by interviews and discussion with ten cybersecurity specialists from two similar MSSPs performing security operations we had the framework validated and, through sense-making of empirical evidence this is the result.

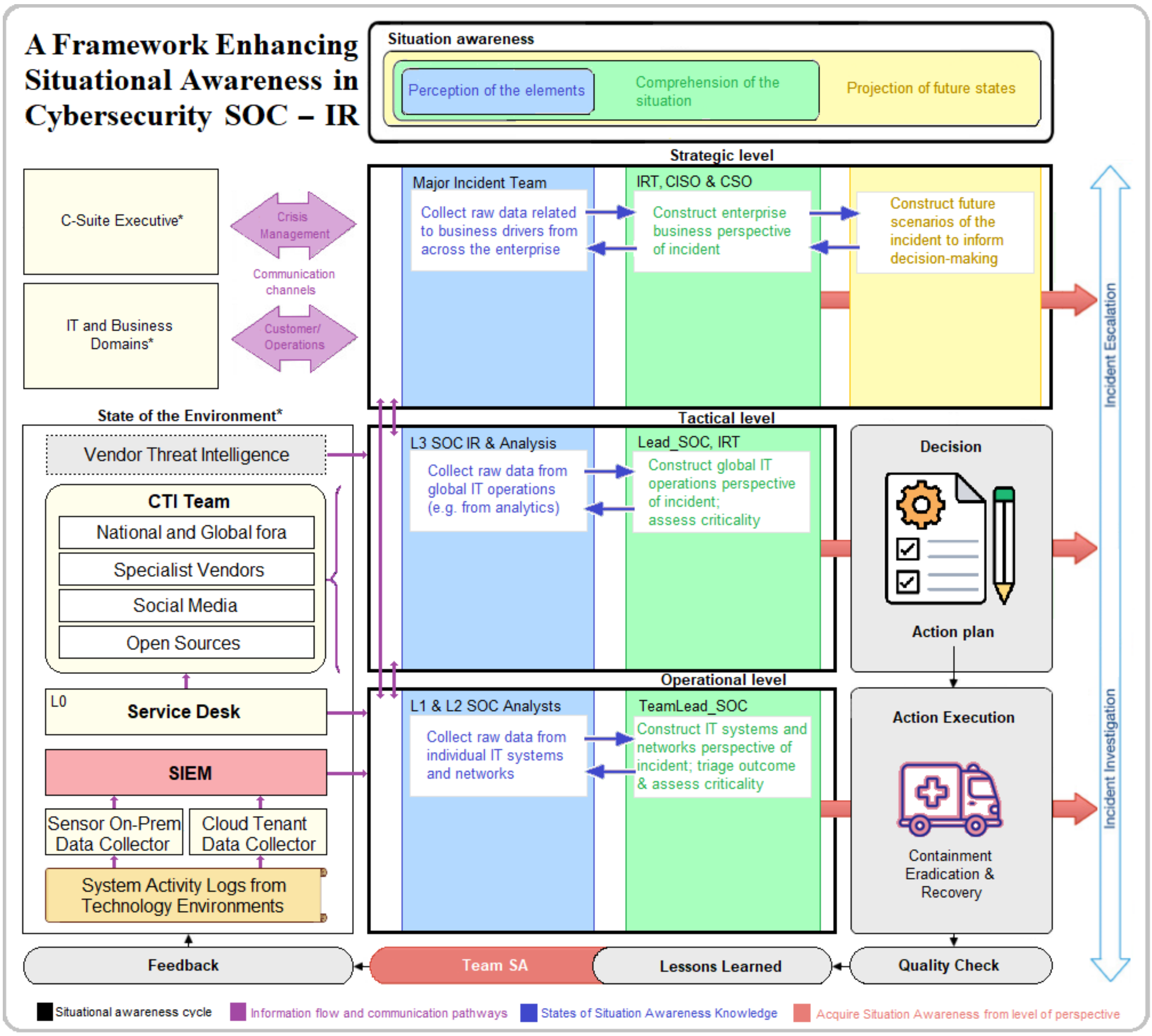

A Framework Enhancing Situational Awareness in Cybersecurity SOC – IR
Situation awareness
Perception of the elements
Comprehension of the situation
Projection of future states
Strategic level
C-Suite Executive*
Crisis Management
Communication channels
IT and Business Domains*
Customer/ Operations
Major Incident Team
Collect raw data related to business drivers from across the enterprise
IRT, CISO & CSO
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Incident Escalation
State of the Environment*
Vendor Threat Intelligence
CTI Team
National and Global fora
Specialist Vendors
Social Media
Open Sources
Tactical level
L3 SOC IR & Analysis
Collect raw data from global IT operations (e.g. from analytics)
Lead_SOC, IRT
Construct global IT operations perspective of incident; assess criticality
Decision
Action plan
L0
Service Desk
SIEM
Sensor On-Prem Data Collector
Cloud Tenant Data Collector
System Activity Logs from Technology Environments
Operational level
L1 & L2 SOC Analysts
Collect raw data from individual IT systems and networks
TeamLead_SOC
Construct IT systems and networks perspective of incident; triage outcome & assess criticality
Action Execution
Containment Eradication & Recovery
Incident Investigation
Feedback
Team SA
Lessons Learned
Quality Check
Situational awareness cycle
Information flow and communication pathways
States of Situation Awareness Knowledge
Acquire Situation Awareness from level of perspective

Figure 5.1: A Dynamic Framework Highlighting Situation Awareness in Cyber IR

The framework within the organizational levels 'operational, tactical and strategic', is modeled as a two-dimensional artifact. Cybersecurity stakeholders are modeled across the vertical dimension representative to each of their levels as inspired by Ahmad et al. (2021)'s case unit (2.7.3) and 'Situation Awareness' as of Endsley (1995)'s process model (2.7.1) for human cognition is modeled across the horizontal dimension. Also based on Endsley (1995)'s model is the *Situation awareness cycle* (black arrows) which can be recognized from Figure 2.10. While some of the theory-informed dimensions of the framework remain unopposed and unchanged, the analysis identifies some changes and additions:

5.1.1 Operational level

On the operational level, the addition of *TeamLead_SOC* represents i) one of our interviewees (relatable to findings), but also ii) the presence of a team leader on daily operations. While the team leader is indeed a level 2 analyst, which is not a new distinction, the literature refers to L1 & L2 SOC Analysts as one unit of different experience without mention of leadership as described in section (2.7.2). However, the data support the theory that L1 analysts may seek assistance from L2 analysts with their tasks, perhaps implying leadership. Moreover, literature refers to L1 & L2 Analysts as juniors and *L3 Analysts* on the tactical level as seniors - this is not supported by our findings. *MSSP1* and *MSSP2* does not carry these distinctions and a senior operator might as well work on the operational level. Through sense-making with the interviewees we came to the conclusion that perhaps *"FinanceCentral"* are more American-hierarchical in their distinction of members of the SOC. Consequently, findings suggest that *MSSP1* and *MSSP2* are more concerned with closing the gap between operators than dividing them based on seniority and experience to avoid bottlenecks in the "chain of response". *"What I do is I enable level 2 analysts to handle more things themselves, and that is the way we want to work."* Lead_SOC

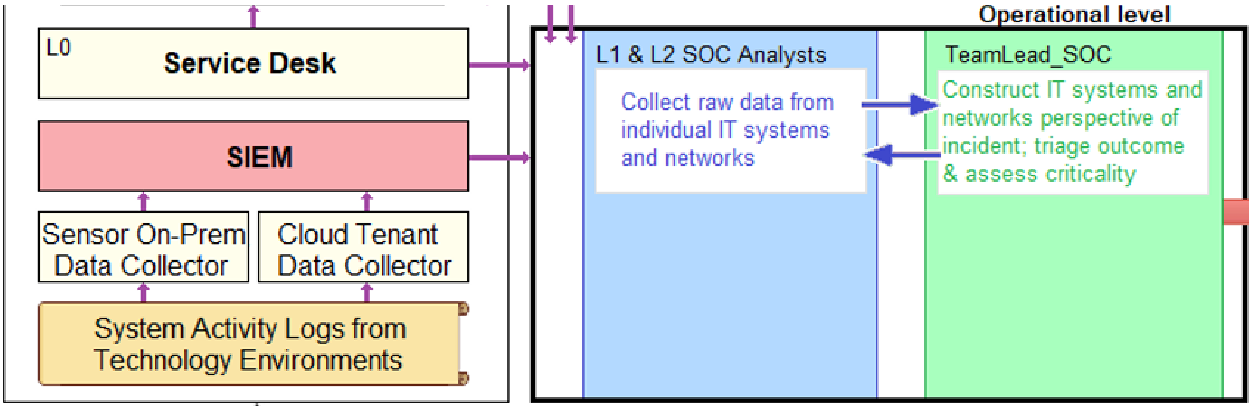

L0
Service Desk
SIEM
Sensor On-Prem Data Collector
Cloud Tenant Data Collector
System Activity Logs from Technology Environments
Operational level
L1 & L2 SOC Analysts
Collect raw data from individual IT systems and networks
TeamLead_SOC
Construct IT systems and networks perspective of incident; triage outcome & assess criticality

Figure 5.2: Operational level dynamics

Another addition to the operational level is to how the analysts perceive the environment. As *MSSP1* and *MSSP2* are both cybersecurity consultancy firms offering security operations and incident response as a service, the "data collection layer" reflecting the 'state of the environment' includes a service desk which work as a platform for customers to promptly reach out if they have issues with their IT systems and networks. For the operational level analysts this means they triage customer tickets alongside SIEM alarms to construct IT systems and networks perspective of incidents. Supporting theory (2.7.2), to triage outcome and assess criticality of incidents, the operational level analysts apply playbooks and use cases developed by *Lead_SOC* and L3 analysts. Newfound data include *the application* of the playbooks and use cases in practice and the course of action taking place should an actionable threat be registered. The use cases are implemented on the SIEM tool to for example track known IOC's. Upon the event of such a use case-trigger, a playbook (set of rules and guidelines) tailored and automated for that specific case appear on the SIEM interface for the analyst to follow. Speeding up the response process from threat observed(perception) -

to threat registered(comprehension) - to making a course of action to either inform about a threat or act upon it to mitigate the risk. When opting to act upon a threat the analysis identifies that at least *MSSP2* initiate an IT Service management (ITSM) process to best integrate with business operations to handle the incident. Basically this means they follow a best-practice framework to perform IT services to customers. If incident triage or predetermined use cases deem a registered threat a certain priority, if something is too big for the operational forum, the incident is rather immediately escalated to the tactical level.

5.1.2 Tactical level

On the tactical level, like *TeamLead_SOC* on the operational level, the *Lead_SOC* represent one of our interviewees. Supporting theory (2.7.2), the *Lead_SOC* recognize his position on the tactical level as an L3 Analyst, leader of the SOC with responsibility for incident response and forensics. While his responsibility was always supported by theory, we had not *named* the role as such in the creation of the conceptual framework. Thus, the distinction *"L3 SOC IR & Analysis"* is also new to the conceptual framework.

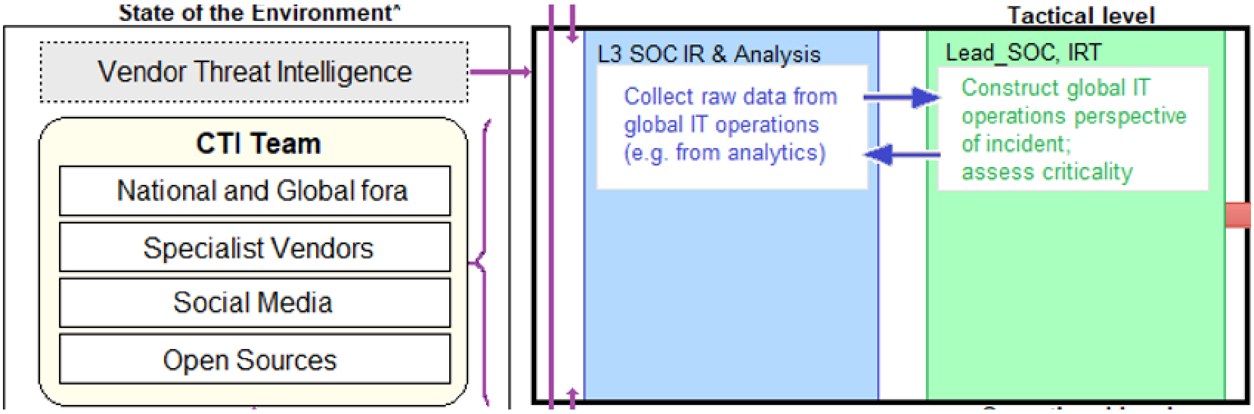

State of the Environment*
Vendor Threat Intelligence
CTI Team
National and Global fora
Specialist Vendors
Social Media
Open Sources
Tactical level
L3 SOC IR & Analysis
Collect raw data from global IT operations (e.g. from analytics)
Lead_SOC, IRT
Construct global IT operations perspective of incident; assess criticality

Figure 5.3: Tactical level dynamics

In the *conceptual* framework (4.1), a vendor of threat intelligence is represented in the "state of the environment" as described by Ahmad et al. (2021) (2.7.3) feeding tactical intelligence to the L3 analysts. Our findings suggest that neither *MSSP1* nor *MSSP2* purchase ready-made threat intelligence from third-party vendors today. They construct their own intelligence and it is up to discussion at least in *MSSP1* whether it is worth investing in ready-made threat intelligence. Thus, the module representing a vendor of threat intelligence in the final framework was "grayed out" with a dotted outline because it was not relevant to represent the studied context. In other contexts this vendor could be relevant as it is a valid option for organizations to make use of vendors of ready-made threat intelligence. Instead, for the purpose of the final framework, the CTI team provides operational, tactical and strategic intelligence to the operational, tactical and strategic levels respectively as of findings from *MSSP2*. Representing this in the final framework, the *CTI Team* has been given a 'curly bracket' of which represents its availability to every level in the hierarchy. While *MSSP1* do not employ a dedicated cyber-threat intelligence team, they do perform its function. Here it is more up to each individual to stay informed about the threat landscape and engage in individual threat hunting.

The data support theory (2.7.2) that the L3 analysts spend most of their time with capability uplift, supporting the operational level with daily operations when they are not handling high-severity incidents. As *Lead_SOC* said, he would much rather spend his time making everyday-work easier for lower level analysts than just being an escalation point. In that respect, the tactical level works as an overlapping connection between the operational and strategic levels. Most days L3 analysts spend their time controlling and supporting the operational level, but if for example an alert classifies malicious activity, it is escalated to the team on the tactical level that coordinates IR and forensic activities with the owners of the involved IT assets. In rare cases of major incidents, the L3 analysts may support the major incident team with global IT operations perspective of the situation along with the necessary resources for that specific incident. While the purple arrows "Information flow and communication pathways" may illustrate this sufficiently between the levels, Figure 5.3 is a good representation of the tactical level dynamics.

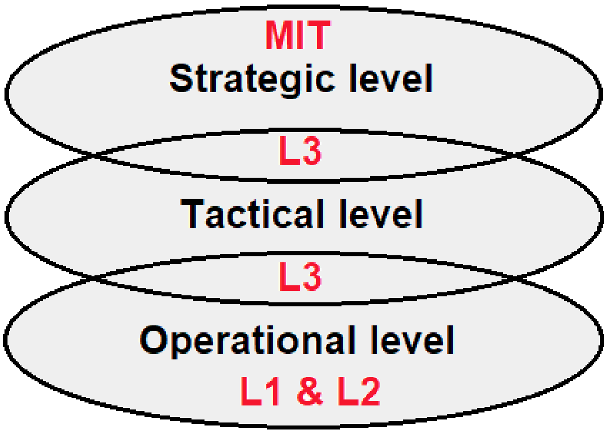


Figure 5.4: SOC-IR dynamics

Should a major incident occur and be observed on either the SIEM through sensors or through the service desk from a customer SOS (or both), the first respondent (typically on the operational level) immediately escalate the incident to the tactical level. In doing so, the *L1 & L2 analysts* call the first line responsible on the security team. *"And this really goes very fast"* as *Lead_ Onboarding* added on the subject. The security team, lead by e.g. *Lead_ SOC* thus performs a routine assessment to quickly acquire the necessary information. Drawing on tactical CTI and raw data from global IT operations, the L3 analysts - based on criteria, assess if the incident classifies as a crisis. If it does, the security team proceeds to contact a dedicated emergency manager (EM), escalating the incident to the strategic level. As of findings from *MSSP1*, the *EM*-role is rotated among equipped designated personnel who are available twenty-four-seven and should always be just one phone-call away.

5.1.3 Strategic level

The *EM* thus owns the incident and sets up a crisis team. Based on both the inquired organizations and, especially *MSSP1*'s classifications (MI1, MI2 etc.), we have called this the "Major Incident Team" (MIT). The *MIT* sits on the strategic level, similar to Ahmad et al. (2021)'s Security leadership team(*SecurityLT*) as can also be found in the conceptual framework (4.1). To set up the team, the *EM* proceeds to create a case in what the *CISO* refers to as the Cyber Security Management System (CSMS), which is a management-approach to streamline processes, responsibilities and governance in such a crisis event. This supports the theory (2.7.3) in that the *SecurityLT* initiates a formal 'managed incident' process which comes with a dedicated technical incident recovery manager similar to the *EM*. Based on our findings, the *EM* here defines who are crisis leader of the situation, who are information manager and who are the technical leader. Theory describes (2.7.3) a *SecurityLT* formed on-the-fly depending on the needs to address the incident, but mentions a cyber operations leader, a SOC leader and the conditional inclusion of a cyber strategy leader, a designated liaison from the CTI team and other L3 analysts. Our findings support this [on-the-fly] formation depending on which resources are necessary for the particular incident, and arguably the permanent roles are also similar given different names. *Lead_ Onboarding* described how they "drum together" all the people they need to meet a challenge [incident] and described a number of people including those in server and network, backup, file and storage *"(...) and of course the incident response team"*. There is really no correct answer as to how the whole of the major incident team should be set up. It all depends on the type of incident beyond the permanent roles. L1 or L2 analysts for example, can have main responsibility for a specific customer (as they are consultants), and if that customer have an incident, then that analyst may be included in the upper levels (MIT). Because, meanwhile they have limited experience and very basic perspective of the 'general' operational environment, they may have very specific data and information; and situation awareness; for that specific customer. And thus, even an operational level analyst could be part of such a major incident team.

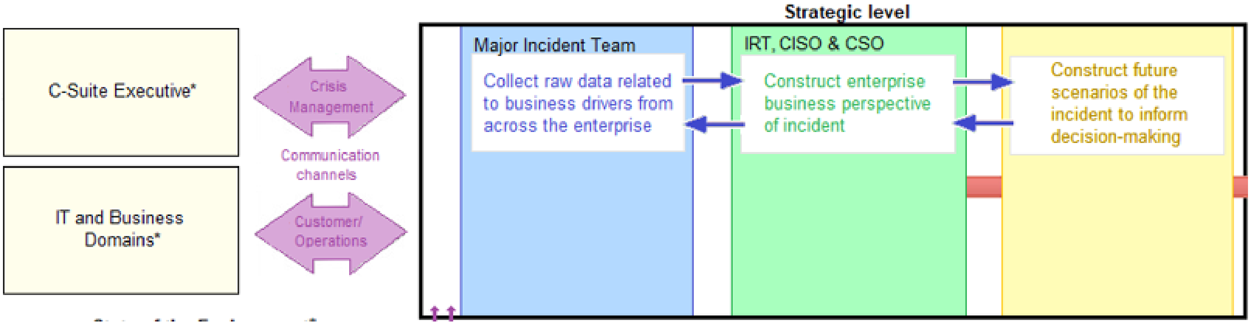

Strategic level
C-Suite Executive*
IT and Business Domains*
Crisis Management
Communication channels
Customer/ Operations
Major Incident Team
Collect raw data related to business drivers from across the enterprise
IRT, CISO & CSO
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making

Figure 5.5: Strategic level dynamics

After setting up the team, based on our findings, the *MIT* sets up communication channels to best coordinate the handling of the incident. One leadership channel for the *MIT* itself and one channel for customer information. This supports theory (2.7.3), whereas Ahmad et al. (2021)'s *SecurityLT* uses communication platforms which they call "bridges" to coordinate a major incident. One management *bridge* for the leadership team and one operational *bridge* to leverage communication to IT and business domains of *"FinanceCentral"*. In *MSSP1* and *MSSP2* however, the channels have some different functionality depending on the situation, while naturally as *Lead_ SOC* mentioned; the 'customer' could well also be their own organization. As they are both consultancy companies, the operations channel setup is conditional to the customer and their needs. Like *Lead_ SOC* also explained: "*If we have a concrete security incident that has happened (with a customer), we integrate with the operational processes that the customer has - because the point is, in very many cases, we are not only the ones who say that "we have seen an incident"[SOC-as-a-service], we are also the IT department of the customer - handling the incident [IRT-as-a-service]*". Hence, if the customer pays for and relies on "the full service" of *MSSP1 MSSP2* as an end-to-end provider, the customer channel is more of a 'channel for customer information'. In such a case, the consulting organization may even be the 'owner' of the IT asset under attack, where as the customer outsource their services (e.g., cloud systems). I.e., the channel is there to inform about the progress towards getting them back to normal operations, for example. On the other side, if the customer operates their own IT domains retaining their own CISO, the procedure is different. In such a case, the customer channel is an operations channel typically used for the same purpose as in the theory (2.7.3); for delegation of the customers IT and business domains to draw on resources and coordinate operations: *"leveraging formal communication protocols to compel technology domain heads of IT as well as the heads of business domains to engage with the incident response process"* (Ahmad et al., 2021). Both *doing*, and *delegating* what to do. Similarly, the senior executive and potential CISO of the *under-attack-organization* would be included in the crisis management channel to convey decisive information and obtain sign-off on important decisions as they are the owners of the involved IT assets, ultimately with the power to decide. Should there be an internal (major) incident (on *MSSP1/MSSP2*'s own systems), findings suggest that coordination procedures are quite similar to those of theory (2.7.3); including the organization's own IT-business domains and C-suite executive to engage in knowledge sharing about the incident and its changing context to inform decision-making. Hence the communication channels are not to customer domains but to internal domains of the respective organization. These different functionalities are represented by an asterisk (*) on both the domain figures in the final framework.

In *"FinanceCentral"* (2.7.3), the CISO has oversight over the entire cybersecurity operations and acts as the communication conduit with the firm's senior executive through the management channel. Our findings suggests that this is not the case in *MSSP1* and *MSSP2* on both external and internal incidents. Here, the IRT and *Lead_IRT* fulfill this role. The IRT are specialized to handle cybersecurity incidents and are trained in communicating with business leaders. The *CISO* - and additionally the *CSO* - instead assist with strategic; legal, business and marketing advice along with the IRT on the *MIT* and to customers through the management channel. We find these distinction probably related to the fact that once again *MSSP1* and *MSSP2* are cybersecurity specialist firms whilst *"FinanceCentral"* in turn are a financial organizations with less cybersecurity resources.

Having acquired an holistic perspective of the incident situation and constructed future scenarios of the incident to inform decision-making, the *MIT* in collaboration with the concerning parties make a *Decision* resulting in an *Action plan.* Putting the decision into effect, the *IRT* initiate '*action execution*' following the incident response cycle, proceeding to execute containment, eradication & recovery to resolve the situation, drawing on the necessary resources. Referring to the framework (5.1), these elements (decision & action execution) are merely generic representations of the pattern of action relatable to Endsley (1995)'s *process model of 'Situation Awareness'* (Figure 5.6 below) and serves its purpose to illustrate the generic next step of the incident response.

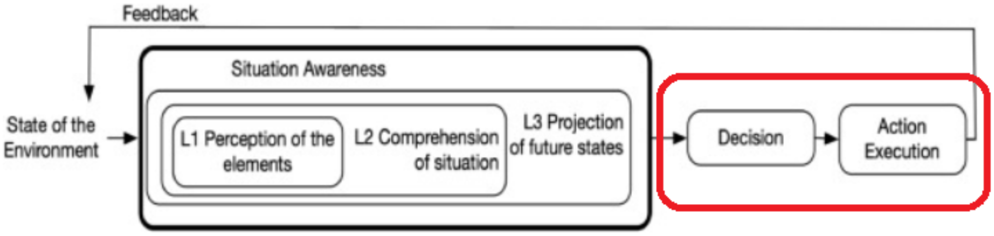

Feedback
Situation Awareness
State of the Environment
L1 Perception of the elements
L2 Comprehension of situation
L3 Projection of future states
Decision
Action Execution

Figure 5.6: 'Situation Awareness' process model (Endsley, 1995)

Excerpt from chapter 2.7.1

'Decision' and 'Action Execution' are stages that are separate from the 'Situation Awareness process' but follow from it as part of the larger process model of human cognition (Ahmad et al., 2021). Hence, SA exists as a facilitator for decision-making rather than part of it. I.e., SA is produced as input for decision-makers deciding how to react to a situation (Evesti et al., 2017). Thus, the 'Decision'-stage is where the operator makes a course of action based on the SA knowledge constructed during the 'Situation Awareness process'. Consequently, 'Action Execution' is where the operator puts the decision into effect based on the previous

stage to continuously change the state of the environment (Ahmad et al., 2021). This decision or choice of action leans on strategical SA knowledge constructed in the projection state relative to Endsley's model (Evesti et al., 2017). The final stage ('Feedback') imposes the course of action and impacts the real world which is ultimately perceived by the operator through its Situation Awareness all over again (Ahmad et al., 2021).

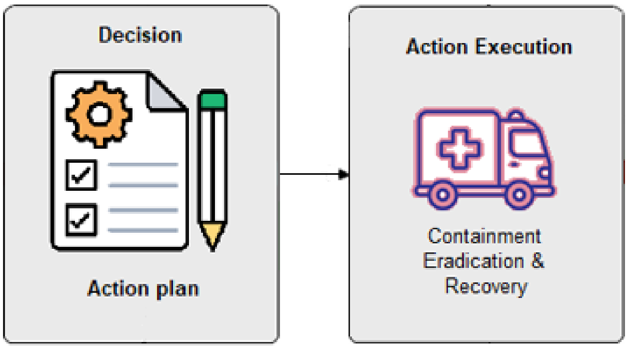


Figure 5.7: Decision & Action Execution

As a decision is made and the action plan is carried out, *TeamLead_SOC* asked and answered: *"Do you really have it all figured out? - what one decision will lead to versus another? You don't know that until it happens, right? And that - is the awareness you should have when making a decision, but it is deficient because not enough people practice making that decision".* – And this is what takes us to the last stage of the SA process (see Figure 2.10); the 'Feedback' which imposes the course of action and impacts the state of the environment which ultimately is perceived by the analyst following the 'Situation Awareness cycle'. On that subject, the *Lead_IRT* made some important remarks of which we have included in the final framework (5.1) to enhance the impact of the SA acquired from the *situation awareness cycle*.

5.1.4 The aftermath

In related work (2.3.3), the systematic study by Vielberth et al. (2020) emphasized that no SOC-specific scientific publication deals with the topic of "post-incident activity" when explaining the incident response life cycle. Deeming literature incomplete, we recognized a research gap in the existing literature. However, we assumed the post-incident activity within CSIRTs to be similar or the same as that of security operations teams. Even though Endsley (1995) includes the 'feedback' in the 'Situation awareness process'(2.10), it says nothing about reflection but rather it is about the impact of the decision that has been made - to the environment. Ahmad et al. (2021) mentions briefly (in section 2.3.3) about a follow-up phase allowing for reflection on the incident handling experience where 'lessons learned' are incorporated into standard operating procedures, but speaks nothing of its relevance to the SOC operations team or SA.

Now, through empirical inquiry, we have found our assumptions to be quite accurate regarding the post-incident activities within CSIRTs to be similar or the same as that of security operations teams. Both the inquired organizations incorporate 'lessons learned' in standard operating procedures after an incident occurs like it is described in theory (2.3.3). After an incident, it is critical that that you assess the situation to determine whether you did the right thing; was it completed in a timely manner; did you have the optimal mechanisms in place to solve it; and so on. *Lead_IRT* mentioned these mechanisms and made the comment that he would like to see a quality assurance phase after the 'action execution'-stage of the conceptual framework, before the feedback onto the environment. He also implied that it should be a separate stage before 'lessons learned'. This is what we have called 'Quality check' in the final framework as you can see of the figure below (Figure 5.8), which results are brought in to the lessons learned for reflection.

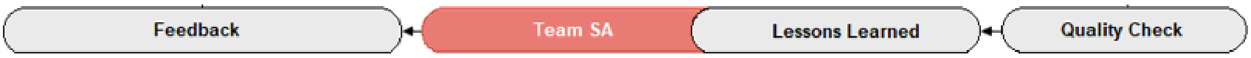


Figure 5.8: The aftermath

While quality check or quality assurance in some respect is already part of lessons learned in theory (2.3.3), we wanted to distinguish this step from 'lessons learned', separating the 'analysis of the incident' (quality check) from the 'reflection of the incident' (lessons learned). The point is that meanwhile these could have been combined into one stage in the framework (5.1), it is first during the lessons learned meeting that the security operations team discuss and reflect upon an incident, together, constructing *Team SA*. Rajivan and Cooke (2017) describes the concept of Team SA as members of a team becoming aware of different aspects of a situation and *knitting the pieces of the puzzle together* through communication or other interactions when dealing with an incident. Our opinion is that members of a team should also become aware of different aspects of a situation after it has occurred, *"untangling the puzzle and turning its pieces to reveal its backside"*. We argue that operators undoubtedly could be informed about some aspect of a situation of which they were not aware of before - during the 'lessons learned' of which would increase their situation awareness. "Were we duly informed of the relevant elements in the environment for the particular situation?; Did we properly understand the context of the situation - on every level?" Thus, as part of the feedback onto the environment is a reflection of the acquired SA from each perspective as illustrated in figure 5.1, representing *the team's* increased knowledge of the current operational picture. The next time an incident of similar nature occur, the reflected SA knowledge sees the entire team more resilient with better awareness of the environment resulting in improved cybersecurity readiness.

Chapter 6

Conclusion

The purpose of this exploratory study was to develop an understanding of the concept of SA and its relation to cybersecurity; investigate its function in the context of enterprise MSSP security operations and examine how SA knowledge is constructed through the organizational levels of the enterprise response. To accomplish this—on a high level, we have provided an empirically validated framework which models how MSSPs are operationalized in cybersecurity operations detection & response. The framework models the communication behavior between cybersecurity stakeholders and conditional internal and external parties to coordinate the management of cybersecurity operations. Following the 'Situation awareness cycle' the MSSP reflects the state of the environment through a socio-technical system of which influences the SOC through its SIEM, CTI team and Service desk. With emphasis on SA, the framework shows how technology, people and processes either support or engage in the perception, comprehension and projection of the operational environment to construct SA knowledge across organizational levels in order to make informed decisions. The framework replicates how SA exists as a facilitator for decision-makers as the SA knowledge constructed and acquired from each level of perspective during the SA process influences the formulation of an action plan which initiates the execution of a decision through the incident response life cycle 'containment eradication & recovery'. Furthermore, the framework accounts for the activities held post-incident to reflect upon the enterprise response, which we argue allows for the construction of team SA. Completing the SA cycle, the final stage 'feedback' imposes the course of action and impacts the state of the environment which is ultimately perceived by the MSSP through its *Situation Awareness* all over again.

Going more into detail, the key findings below summarize our conclusion through its addressing of the research problem:

Key findings

- In 'best practice' MSSPs, reflecting the state of the environment are "on-prem" physical sensors and cloud tenants that are placed within the customer's own systems transferring system activity logs from internal and external technology environments. The syslogs are channeled through data collectors directly into the SIEM platform which correlate and accumulate the data allowing for visualization. Allowing for analysts to sense the environment. Simultaneously, MSSPs employ service desks of which allows for customers to reach out should an incident occur that is for example not picked up by the SIEM. For the operational level L1 & L2 SOC analysts this means they triage customer tickets alongside SIEM alarms to construct IT systems and networks perspective of incidents. This is a key finding to how operational level analysts perceive the environment in MSSPs. Another way for the SOC and security analysts to stay up to date with the operational environment is through the CTI team which collect threat intelligence data using tools like Feedly to construct actionable CTI. Neither of the inquired organizations subscribe to ready-made threat intelligence from specialist vendors, yet it remains a valid option for organizations to adopt as at least *MSSP1* uttered a desire to pay for these services, but was hold off due to monetary reasons. Thus for MSSPs, the vendor presented in the final framework is still significant.

- In MSSPs, the operational level analysts triage outcome and assess criticality of incidents observed and registered through the SIEM and the service desk using playbooks and use cases developed by tactical level analysts. As a result, L1 & L2 analysts construct IT systems and networks perspective of an incident. Should an incident prove a false positive, or for example turn out to be "relevant but not critical", the analysts simply informs the stakeholder of the assessed environment about the perceived threat. When opting to act upon a registered low-severity threat they initiate an 'IT Service management (ITSM) process' to best integrate with customer operations to handle the incident. Basically this means that MSSPs follow best-practice frameworks to perform services for customers. If incident triage or predetermined use cases deem a registered threat a certain high priority; if something is too big for the operational forum, the incident is rather immediately escalated to the tactical level.

- On the tactical level, L3 analysts perceive the environment through incidents escalated by global operations (e.g. the operational level) or through tactical threat intelligence from the CTI team. L3 analysts spend most of their time controlling and supporting the operational level, but if for example an alert classifies malicious activity, it is escalated to the team on the tactical level that coordinates IR and forensic activities with the owners of the involved IT assets. Should a major incident occur and be observed through the operational and tactical level it is the job of *Lead_ SOC* to coordinate with the emergency manager to trigger the formation of the major incident response team. In such rare cases, the L3 analysts may support the MIT with global IT operations perspective of the situation along with the necessary resources for that specific incident.

- On the strategic level, MSSPs retain an EM who owns and is responsible for the management of the major incident. The EM-role is rotated among designated equipped personnel which are part of the MIT. To set up the team and formally escalate the incident the EM creates a case in CSMS, which is a management system applied by MSSPs to govern crisis events. Subsequently he defines the roles critical to the handling of the incident before establishing communication channels to all stakeholders concerned with the incident which allows for the coordination of the response across knowledge areas. In large scale MSSPs, the IRT has oversight over the entire cybersecurity operations and acts as the communication conduit with C-suite executives through the management channel. The IRT are trained to communicate with business leaders and are in the context of MSSPs (especially) specialized in dealing with cybersecurity incidents. A financial organization with an in-house SOC for example would refer to an IRT as part of their SOC team, whilst the IRT in MSSPs are the "stars of the operation" who are only called in for the most critical missions. The CISO and CSO operate on a higher level in MSSPs, assisting with strategic; legal, business and marketing advice along on the MIT and to C-suite executives through the management channel. Having acquired an holistic perspective of the incident situation, the MIT in collaboration with the concerning parties leverage an action plan of which they integrate with business and IT operations at the customers location to start drawing on resources to handle the incident (of which can be entirely different depending on the scenario, thus the framework addresses a generic scenario following the incident response life cycle).

- Guided by the SA cycle and IR life cycle, MSSPs incorporate a quality check following the conclusion of an incident. The quality check is incorporated to analyze the performance of the incident detection and response, to assess whether the right choices were made. In the subsequent lessons learned, the security teams discuss and reflect upon their performance in a plenary format. In this context we argue that the different security teams (separated by organizational levels) have acquired different perspectives of SA of which they accumulate to construct Team SA through the collective of a lessons learned meeting. Completing the framework, the final stage ’feedback’ imposes the course of action and impacts the state of the environment which is ultimately perceived by the MSSP team through its *Situation Awareness* all over again.

6.1 Contribution to theory and industry

Our work contributes to situation awareness theory in the context of cybersecurity operations and incident response by advancing the understanding of the organizational capabilities of MSSPs to develop situation awareness of the cyber-threat landscape and to manage the broader operational dynamics. By introducing the empirically validated dynamic framework enhancing situation awareness in cybersecurity SOC—IR we expand on existing models of situation awareness. Through Endsley (1995)’s *’Situation Awareness’ process model* for human cognition that is framed from an information-processing perspective we use the logic of an operators ’state of knowledge’ that can exist at three different level states in a larger context and for expanded use, which collectively leads to the making of a decision and action execution. Following, the framework improves on Endsley’s concept of ’feedback’ where we argue assessment of the decision-making process allows for improved impact of its influence onto the environment. As for Ahmad et al. (2021)’s process model *Situation awareness in Cybersecurity IR* we apply its dynamic behavior processes to an MSSP cybersecurity operations and IR context and expand its function to a broader operational environment including conditional parties (e.g., external domains through the communication channels). Using Ahmad et al. (2021)’s case unit of *Information flow and communication pathways* we interpret and bring to life a flow diagram to replicate the organizational structure of a cybersecurity SOC-IR team. Through the combination of all the models, scrutinized and validated through discussion and input with cybersecurity specialists we have been made able to propose a conceptual framework which represents the workings of cybersecurity operations teams in the context of MSSPs to construct SA knowledge.

For industry, our work on account of our interactions with cybersecurity specialists, brings to life the best practices applied for large scale enterprise MSSPs and enlightens the dynamics within such processes when it comes to cybersecurity operations. The framework in this respect reflects guiding practices for organizations to apply in the formation of similar cybersecurity operation teams. Even for organizations outside the MSSP business, this framework can provide insights or guidelines towards raising awareness in operators through generalizing the processes that allow for the construction of SA. Furthermore, it may prove helpful for organizations opting to outsource such operations to understand the services they are provided. Lastly, we create opportunities for organizations to benchmark their operations and compare themselves with best practice MSSPs to improve on operating procedures.

6.2 Limitations and opportunities for further research

First, given a larger network of connections, we could have broadened the population of enquiry to include participants from a greater number of relevant organizations. This would allow for a more saturated perspective and a broader understanding of the subject in question. Given more time we could have expanded the scope of our investigation to for example include non-IT personnel in order to gain a broader understanding of enterprise situation awareness and investigate the interactions between cybersecurity and non-cybersecurity personnel during incident response.

Second, although our study is grounded in theory (i.e our selected interpretation of the concepts of cybersecurity operations and SA were developed from elements of Ahmad et al. (2021)'s process model and case unit, and Endsley (1995) logic), there are various theories of situation awareness and IR dynamics that could have been examined and used to improve upon the quality of the overall theoretical contribution. Also, through our research we realize there are things we could explore further. While our study explored some aspects of for example information sharing, we could have expanded our scope to include sharing of situation awareness knowledge across organizational boundaries, i.e. inter-organizational; distributed; SA. But we did not have neither the time or resources to pursue this. By pursuing this angle, we would investigate how organizations communicate with one another and what channels they use to do so for example.

Third, interviewing people who work in cybersecurity, the respondents may not be able to provide an adequate answer as the information they have could be sensitive. Following our interviews we found there was a lot of content of which could not be presented in the empirical findings. It would be interesting to approach this study through action research for example and reflect on own practices to contribute to this work.

Lastly, given the nature of the organizations that were investigated in this exploratory study, a key limitation is the lack of generalization. The inquired organizations are large scale and ultimately specialized in cybersecurity services (MSSPs), thus for smaller and less capable organizations the dynamics and capability requirements of the framework could be too complicated and could differ substantially from that of e.g., an SME context. Thus, by expanding this work to include a broader range of organizational contexts, as the fewest of organizations are of the size of LSE, one could improve the overall applicability of the framework and significantly contribute to theory on the subject.

Appendix A

Interview Questions

Del 1: Generell informasjon om deg og organisasjonen

1) Hvilken rolle og arbeidserfaring har du i organisasjonen?
2) Hva er dine arbeidsoppgaver på dagsbasis?
3) Hva er dine tanker om situasjonsbevissthet?
4) Har du tatt del i noen relevante prosjekter om situasjonsbevissthet?
5) Hvordan vil du karakterisere bedriftens type forretningsvirksomhet?
6) Hvor lenge har dere vært i denne bransjen?
7) Hva slags kunder har dere?
8) Har dere noe statistikk på antall hendelser mot dere selv eller kundene deres? f.eks. antall cybersikkerhet-hendelser per dag/uke/måned/år?

Del 2: IT og Cybersikkerhet

1) Vi vet at dere bruker en SIEM-løsning for å håndtere hendelsesdata. Hvilken leverandør eller teknologi bruker dere, og hvorfor har dere valgt spesifikt denne?
2) Kan du fortelle litt om strukturen rundt SIEM plattformen?
3) Hvem opererer SIEM plattformen og oppfatter dataene for å danne forståelig/brukbar informasjon for tolkning av ledere og beslutningstakere/ potensielt ikke-teknisk forstående?
4) Har dere et trusseletteretnings-team eller noen som utfyller en slik rolle?
5) Benytter dere også en 'leverandør' av trusseletterretning?
6) Er dere del av et informasjonsdeling-nettverk sammen med andre bedrifter eller funksjoner for å dele og motta informasjon om trusler og potensielle hendelser?
7) Bruker du eller dere andre former for ekstern informasjonsdeling for å få gjort jobben deres?

Del 3: Ved en sikkerhetshendelse

1) Hva ser du på som de største utfordringene knyttet til en cyber-sikkerhetshendelse?
2) Ut i fra din rolle; hvis det oppstår en sikkerhetshendelse, hva sier retningslinjer og protokoller om hva du skal gjøre da?
3) Hvordan sørger dere for at de ansatte tar lærdom av oppståtte cyber-sikkerhetshendelser?

Del 4: Kan du følge oss gjennom bedriftens prosess for hendelses-respons på en alvorlig cyber-sikkerhetshendelse; fra start til slutt?

Vi ønsker å skape en dialog her. I og med at dette er et semistrukturert intervju er vi klare med oppfølgingsspørsmål ettersom du eventuelt forklarer om de forskjellige prosessene.

Del 5: Rammeverket og situasjonsbevissthet

Vi vil presentere vårt rammeverk, forklare litt rundt teorien og hvordan rammeverket skal tolkes. Gjennomgangen tar ca 3 minutter før vi ønsker å få validert vår tolkning av hvordan hendelseshåndtering i SOC fungerer samt hvordan situasjonsbevissthet oppfattes og informasjonsflyt foregår blant de ansatte. Likeså ønsker vi her å skape en dialog, og gjerne en diskusjon rundt rammeverket som kan løpe ut tiden av intervjuet.

Appendix B

Interview Guide

Takk for at du deltar i dette intervjuet med oss. Hensikten med dette intervjuet er å undersøke situasjonsbevissthet innen hendelseshåndtering, praksis brukt for å oppnå dette, og hvordan dette gjennomføres for å øke bevisstheten hos de ansatte. Målet med intervjuet er å forstå hva som er praksis for så å potensielt finne ut hva som er beste praksis basert på deres kunnskap og den kunnskapen vi har opparbeidet oss i løpet av vår litteraturgjennomgang. Vi vil også, med samme formål, sammenligne deres praksis med andre intervjuobjekters praksis. Intervjuet vil derfor både forsøke å validere den forståelsen vi har for disse praksisene, samt også stille spørsmål for å utfylle de eventuelle mangler vi har i vår kunnskap. Vi ønsker også å validere et rammeverk som vi har utviklet som tar for seg situasjonsbevissthet innen hendelseshåndtering.

Dette intervjuet er anonymt. Vi vil IKKE skrive noe personlig informasjon om intervjuobjektet. Eventuelle personlige opplysninger vil ikke bli transkribert eller lagt til i dokumentet, og alle opptak vil bli slettet ved slutten av hovedleveransen, beregnet dato: 03.06.2022. Intervjuobjektet står fritt til å nekte å svare på spørsmål uten å gi grunnlag for dette. Intervjuobjektet forstår at dette intervjuet og informasjon innhentet fra det, vil bli brukt i masteroppgaven "A Dynamic Framework Enhancing Situational Awareness in Cybersecurity Incident Response for Enterprises" og gir samtykke til studentene ved UiA under Master: Cybersikkerhet ledelse: Jarl Andreassen og Martin Eileraas, å bruke intervjuet og ta opp i masteroppgaven deres.

Intervjuet er semistrukturert og vil stille spørsmål om hvordan den ansatte har opplevd sikkerhetspraksis, om de har en viss forståelse av situasjonsbevissthet, og hvordan dette påvirker deres organisasjon og hvor godt visse praksiser fungerer for organisasjonen og den ansatte.

Det er ønskelig at vi klarer å holde oss litt innenfor temaet som diskuteres med en viss vekt på å være kort og konsis - med all respekt :)

Estimert tid for dette intervjuet er 50 minutter.

Del 1: Generell informasjon om deg og organisasjonen

1) Hvilken rolle og arbeidserfaring har du i organisasjonen?
2) Hva er dine arbeidsoppgaver på dagsbasis?
3) Hva er dine tanker om situasjonsbevissthet?
4) Har du tatt del i noen relevante prosjekter om situasjonsbevissthet?
5) Hvordan vil du karakterisere bedriftens type forretningsvirksomhet?
6) Hvor lenge har dere vært i denne bransjen?
7) Hva slags kunder har dere?
8) Har dere noe statistikk på antall hendelser mot dere selv eller kundene deres? f.eks. antall cybersikkerhet-hendelser per dag/uke/måned/år?

Del 2: IT og Cybersikkerhet

1) Vi vet at dere bruker en SIEM-løsning for å håndtere hendelsesdata. Hvilken leverandør eller teknologi bruker dere, og hvorfor har dere valgt spesifikt denne?
2) Kan du fortelle litt om strukturen rundt SIEM plattformen?
3) Hvem opererer SIEM plattformen og oppfatter dataene for å danne forståelig/brukbar informasjon for tolkning av ledere og beslutningstakere/ potensielt ikke-teknisk forstående?
4) Har dere et trusseletteretnings-team eller noen som utfyller en slik rolle?
5) Benytter dere også en 'leverandør' av trusseletterretning?
6) Er dere del av et informasjonsdeling-nettverk sammen med andre bedrifter eller funksjoner for å dele og motta informasjon om trusler og potensielle hendelser?
7) Bruker du eller dere andre former for ekstern informasjonsdeling for å få gjort jobben deres?

Del 3: Ved en sikkerhetshendelse

1) Hva ser du på som de største utfordringene knyttet til en cyber-sikkerhetshendelse?
2) Ut i fra din rolle; hvis det oppstår en sikkerhetshendelse, hva sier retningslinjer og protokoller om hva du skal gjøre da?
3) Hvordan sørger dere for at de ansatte tar lærdom av oppståtte cyber-sikkerhetshendelser?

Del 4: Kan du følge oss gjennom bedriftens prosess for hendelses-respons på en alvorlig cyber-sikkerhetshendelse; fra start til slutt?

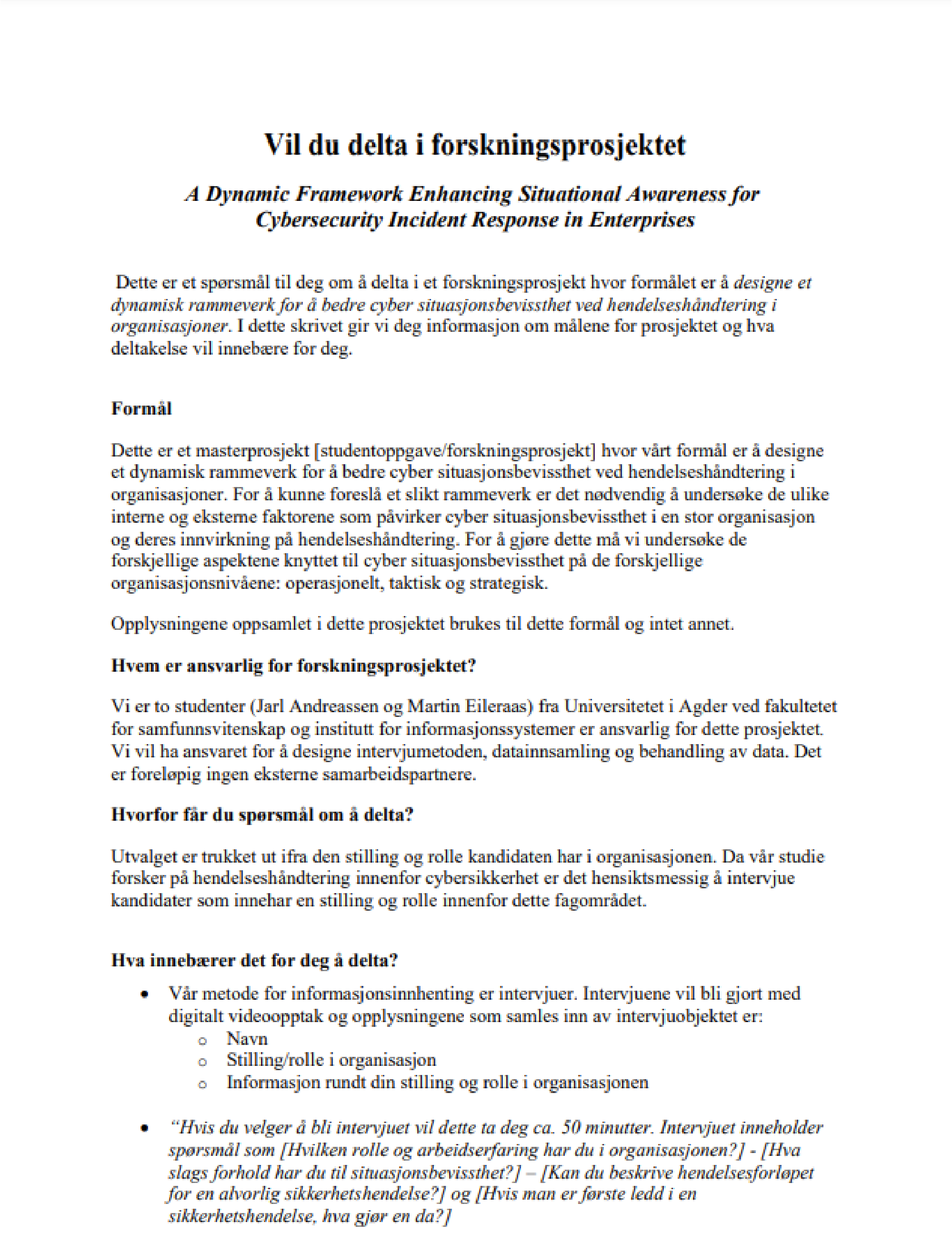
Vi ønsker å skape en dialog her. I og med at dette er et semistrukturert intervju er vi klare med oppfølgingsspørsmål ettersom du eventuelt forklarer om de forskjellige prosessene.

Del 5: Rammeverket og situasjonsbevissthet

Vi vil presentere vårt rammeverk, forklare litt rundt teorien og hvordan rammeverket skal tolkes. Gjennomgangen tar ca 3 minutter før vi ønsker å få validert vår tolkning av hvordan hendelseshåndtering i SOC fungerer samt hvordan situasjonsbevissthet oppfattes og informasjonsflyt foregår blant de ansatte. Likeså ønsker vi her å skape en dialog, og gjerne en diskusjon rundt rammeverket som kan løpe ut tiden av intervjuet.

Appendix C

Consent Form



Vil du delta i forskningsprosjektet

A Dynamic Framework Enhancing Situational Awareness for Cybersecurity Incident Response in Enterprises

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å *designe et dynamisk rammeverk for å bedre cyber situasjonsbevissthet ved hendelseshåndtering i organisasjoner*. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette er et masterprosjekt [studentoppgave/forskningsprosjekt] hvor vårt formål er å designe et dynamisk rammeverk for å bedre cyber situasjonsbevissthet ved hendelseshåndtering i organisasjoner. For å kunne foreslå et slikt rammeverk er det nødvendig å undersøke de ulike interne og eksterne faktorene som påvirker cyber situasjonsbevissthet i en stor organisasjon og deres innvirkning på hendelseshåndtering. For å gjøre dette må vi undersøke de forskjellige aspektene knyttet til cyber situasjonsbevissthet på de forskjellige organisasjonsnivåene: operasjonelt, taktisk og strategisk.

Opplysningene oppsamlet i dette prosjektet brukes til dette formål og intet annet.

Hvem er ansvarlig for forskningsprosjektet?

Vi er to studenter (Jarl Andreassen og Martin Eileraas) fra Universitetet i Agder ved fakultetet for samfunnsvitenskap og institutt for informasjonssystemer er ansvarlig for dette prosjektet. Vi vil ha ansvaret for å designe intervjumetoden, datainnsamling og behandling av data. Det er foreløpig ingen eksterne samarbeidspartnere.

Hvorfor får du spørsmål om å delta?

Utvalget er trukket ut ifra den stilling og rolle kandidaten har i organisasjonen. Da vår studie forsker på hendelseshåndtering innenfor cybersikkerhet er det hensiktsmessig å intervjue kandidater som innehar en stilling og rolle innenfor dette fagområdet.

Hva innebærer det for deg å delta?

- Vår metode for informasjonsinnhenting er intervjuer. Intervjuene vil bli gjort med digitalt videoopptak og opplysningene som samles inn av intervjuobjektet er:
    - Navn
    - Stilling/rolle i organisasjon
    - Informasjon rundt din stilling og rolle i organisasjonen

- *"Hvis du velger å bli intervjuet vil dette ta deg ca. 50 minutter. Intervjuet inneholder spørsmål som [Hvilken rolle og arbeidserfaring har du i organisasjonen?] - [Hva slags forhold har du til situasjonsbevissthet?] – [Kan du beskrive hendelsesforløpet for en alvorlig sikkerhetshendelse?] og [Hvis man er første ledd i en sikkerhetshendelse, hva gjør en da?]*

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun behandlingsansvarlige Jarl Andreassen og Martin Eileraas vil ha tilgang til dine opplysninger.
- Kun behandlingsansvarlige Jarl Andreassen og Martin Eileraas vil samle inn, bearbeide og lagre data.
- Tiltak for at ingen uvedkommende får tilgang til personopplysningene dine inkluderer
  - Navn og annen identifiserbar informasjon vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data. F.eks. «Lead_SOC» for lederen av SOC fremfor navnet til kandidaten.
  - Datamateriale vil bli lagret på sikret OneDrive sky-konto under skolens domene med to-faktor autentisering.
  - Personopplysninger og øvrige sensitive data vil bli lagret separat i innelåst/kryptert mappe

Deltakere vil ikke kunne gjenkjennes i publikasjon. Deltakere vil anonymiseres og refereres til som intervjuobjekt eller f.eks. «Lead_SOC» e.l. dersom det er hensiktsmessig. Organisasjonens navn vil også anonymiseres. I den sammenheng vil ikke informasjon kunne knyttes til deltaker.

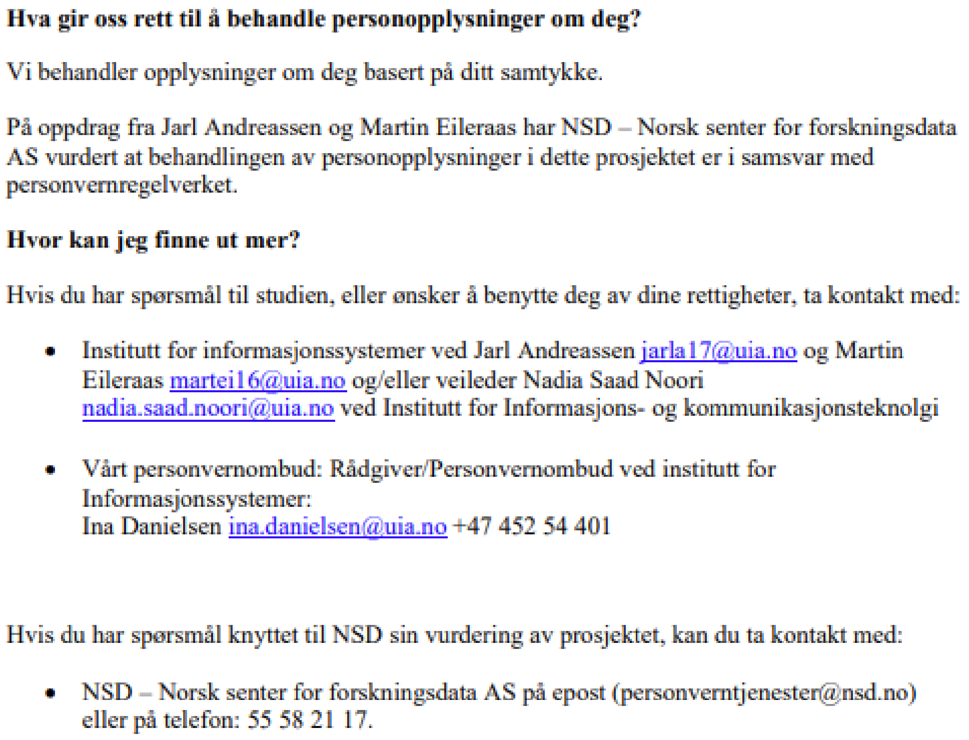
Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Etter endt prosjekt vil alt av oppbevarte data slettes fullstendig fra alle medier.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.



Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Jarl Andreassen og Martin Eileraas har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for informasjonssystemer ved Jarl Andreassen jarla17@uia.no og Martin Eileraas martei16@uia.no og/eller veileder Nadia Saad Noori nadia.saad.noori@uia.no ved Institutt for Informasjons- og kommunikasjonsteknolgi

- Vårt personvernombud: Rådgiver/Personvernombud ved institutt for Informasjonssystemer:
  Ina Danielsen ina.danielsen@uia.no +47 452 54 401

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Jarl Andreassen *Martin Eileraas*

Jarl Andreassen Martin Eileraas

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *A Dynamic Framework Enhancing Situational Awareness for Cybersecurity Incident Response in Enterprises*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i intervjuer
- □ *at Jarl Andreassen og Martin Eileraas kan gi opplysninger om meg til prosjektet*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Bibliography

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L., 2021. How can organizations develop situation awareness for incident response: A case study of management practice. Computers and Security 101, 102122. URL: https://www.sciencedirect.com/science/article/pii/S0167404820303953, doi:https://doi.org/10.1016/j.cose.2020.102122.

Arlitsch, K., Edelman, A., 2014. Staying safe: Cyber security for people and organizations. Journal of Library Administration 54, 46–56. URL: https://doi.org/10.1080/01930826.2014.893116.

Arnborg, S., Brynielsson, J., Artman, H., Wallenius, K., 2000. Information awareness in command and control:precision, quality, utility URL: https://www.csc.kth.se/~joel/iq.pdf.

Barnum, S., 2014. Standardizing cyber threat intelligence information with the structured threat information expression (stix™) URL: http://stixproject.github.io/getting-started/whitepaper/.

Bhatt, S., Manadhata, P., Zomlot, L., 2014. The operational role of security information and event management systems. IEEE Security and Privacy 12, 35 – 41. URL: https://ieeexplore.ieee.org/document/6924640, doi:10.1109/MSP.2014.103. cited by: 76.

Bidou, R., Bourgeois, J., Spies, F., 2004. Towards a global security architecture for intrusion detection and reaction management, in: Chae, K.J., Yung, M. (Eds.), Information Security Applications, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 111–123.

Chopra, M., Mahapatra, C., 2019. Significance of security information and event management (siem) in modern organizations. International Journal of Innovative Technology and Exploring Engineering 8, 432 – 435. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067925104&partnerID=40&md5=3d226f86a78b017f3d1abe12bf4573a7.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer security incident handling guide, recommendations of the national institute of standards and technology, sp800-61r2. URL: http://dx.doi.org/10.6028/NIST.SP.800-61r2.

Conti, G., Nelson, J., Raymond, D., 2013. Towards a cyber common operating picture. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84904402812&partnerID=40&md5=ab7ea633d6c24198da16a5779a76c635.

Conti, M., Dehghantanha, A., Dargahi, T., 2018. Cyber threat intelligence. Springer. URL: https://link.springer.com/chapter/10.1007/978-3-319-73951-9_1.

Cresswell, J.W., 2008. The Selection of a Research Design the Three Types of Designs. URL: https://www.sagepub.com/sites/default/files/upm-binaries/22780_Chapter_1.pdf.

de Fuentes, J.M., González-Manzano, L., Tapiador, J., Peris-Lopez, P., 2017. Pracis: Privacy-preserving and aggregatable cybersecurity information sharing. Computers and Security 69, 127–141. URL: https://www.sciencedirect.com/science/article/pii/S0167404816301821, doi:https://doi.org/10.1016/j.cose.2016.12.011. security Data Science and Cyber Threat Management.

DeCarlo, M., 2021. Qualitative interview techniques URL: https://scientificinquiryinsocialwork.pressbooks.com/chapter/13-2-qualitative-interview-techniques/.

Deloitte, 2019. The future of cyber survey 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf.

Denzin, N.K., Lincoln, Y.S., 2008. Strategies of Qualitative Inquiry. URL: https://books.google.no/books?id=hD7W095U66cC&lpg=PR7&ots=7Y2hn4AnP4&dq=denzin%20and%20lincoln%202008&lr&hl=no&pg=PA4#v=onepage&q&f=false.

DNV, 2022. The three-pillar approach to cyber security: Data and information protection URL: https://tinyurl.com/mtfb2ky6.

Endsley, M., 1995. Toward a theory of situation awareness in dynamic systems. Human Factors 37, 32 – 64. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-0029004440anddoi=10.1518%2f001872095779049543andpartnerID=40andmd5=607061a405660f4f81316a02c00eca17, doi:10.1518/001872095779049543. cited by: 4890.

Evesti, A., Kanstrén, T., Frantti, T., 2017. Cybersecurity situational awareness taxonomy , 1–8doi:10.1109/CyberSA.2017.8073386.

Franke, U., Brynielsson, J., 2014. Cyber situational awareness – a systematic review of the literature. Computers and Security 46, 18–31. URL: https://www.sciencedirect.com/science/article/pii/S0167404814001011, doi:https://doi.org/10.1016/j.cose.2014.06.008.

Gailey, S., 2020. A brief history of siem URL: https://cybersecurity-magazine.com/a-brief-history-of-siem/.

Gartner, 2020. Gartner 2021 cio agenda survey. URL: https://tinyurl.com/574mmh94.

Gartner, 2021. Gartner forecasts worldwide security and risk management spending to exceed 150 billion in 2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem.

Gartner, 2022. Managed security service provider (mssp) URL: https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider.

Given, L.M., 2008. Induction. the sage encyclopedia of qualitative research methods URL: https://methods.sagepub.com/reference/sage-encyc-qualitative-research-methods/n212.xml, doi:https://dx.doi.org/10.4135/9781412963909.n212.

González-Granadillo, G., González-Zarzosa, S., Diaz, R., 2021. Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. Sensors 21. URL: https://www.mdpi.com/1424-8220/21/14/4759, doi:10.3390/s21144759.

Goodwin, C., Nicholas, J.P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Massagli, A., Mckay, A., Mckitrick, P., Neutze, J., et al., 2015. A framework for cybersecurity information sharing and risk reduction. Microsoft URL: https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf.

Griffin, C., 2004. The advantages and limitations of qualitative research in psychology and education URL: https://www.researchgate.net/publication/310480387_The_advantages_and_limitations_of_qualitative_research_in_psychology_and_education.

Hasan, S., Ali, M., Kurnia, S., Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications 58, 102726. URL: https://www.sciencedirect.com/science/article/pii/S2214212620308656, doi:https://doi.org/10.1016/j.jisa.2020.102726.

Hennink, M., Hutter, I., Bailey, A., 2020. Qualitative research methods. URL: https://books.google.no/books?hl=no&lr=&id=_InCDwAAQBAJ&oi=fnd&pg=PP1&dq=Hennink,+M.,+Hutter,+I.,+%26+Bailey,+A.+2020&ots=3uaOmOu-iy&sig=dOW95O8QXWaU4b3tAlWIQz5dSwO&redir_esc=y#v=onepage&q&f=false.

Horneman, A., 2019. Situational awareness for cybersecurity: An introduction. Carnegie Mellon University's Software Engineering Institute Blog. URL: http://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/.

Hydro, 2020. Cyberangrep på hydro URL: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/.

Jajodia, S., Albanese, M., 2017. An Integrated Framework for Cyber Situation Awareness. volume 10030 of *Theory and Models for Cyber Situation Awareness*. URL: https://link.springer.com/chapter/10.1007/978-3-319-61152-5_2#Sec1.

Jasper, S.E., 2016. U.s. cyber threat intelligence sharing frameworks. International Journal of Intelligence and CounterIntelligence 30. URL: https://www.tandfonline.com/doi/full/10.1080/08850607.2016.1230701.

Kakilla, C., 2021. Strengths and weaknesses of semi-structured interviews in qualitative research: A critical essay URL: https://www.preprints.org/manuscript/202106.0491/v1/download.

Kallio, H., Pietilä, A.M., Johnson, M., Kangasniemi, M., . Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of Advanced Nursing 72, 2954–2965. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/jan.13031, doi:https://doi.org/10.1111/jan.13031.

Kent, K., Souppaya, M., 2006. Guide to computer security log management. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

Kitchenham, B., 2004. Procedures for performing systematic reviews. Keele, UK, Keele Univ. 33. URL: https://www.researchgate.net/profile/Barbara-Kitchenham/publication/228756057_Procedures_for_Performing_Systematic_Reviews/links/618cfae961f09877207f8471/Procedures-for-Performing-Systematic-Reviews.pdf.

Kitchenham, B., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering URL: https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.471.

Klevstrand, A., Bugge, W., Christensen, J., Magnus, C.H., 2020. Hackerangrepet mot hydro enda dyrere enn tidligere antatt: Ny prislapp på 800 millioner kroner. *Dagens Næringsliv*. URL: https://tinyurl.com/tj94xjh.

Leszczyna, R., Wrobel, M., 2019. Threat intelligence platform for the energy sector URL: https://onlinelibrary.wiley.com/doi/full/10.1002/spe.2705.

Mitre.org, 2022. The mitre corporation URL: https://www.mitre.org/.

Muniz, J., McIntyre, G., AlFardan, N., 2015. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press.

Myers, M.D., 2021. Qualitative research in information systems URL: www.qual.auckland.ac.nz.

Myers, M.D., Newman, M., 2007. The qualitative interview in is research: Examining the craft. Information and Organization 17, 2–26. URL: https://www.sciencedirect.com/science/article/pii/S1471772706000352, doi:https://doi.org/10.1016/j.infoandorg.2006.11.001.

Naseer, H., Maynard, S.B., Desouza, K.C., 2021. Demystifying analytical information processing capability: The case of cybersecurity incident response. Decision Support Systems 143, 113476. URL: https://www.sciencedirect.com/science/article/pii/S0167923620302311, doi:https://doi.org/10.1016/j.dss.2020.113476.

NSD, 2022. Om nsd - norsk senter for forskningsdata. URL: https://www.nsd.no/om-nsd-norsk-senter-for-forskningsdata/.

Nyre-Yu, M., Gutzwiller, R., Caldwell, B., 2019. Observing cyber security incident response: Qualitative themes from field research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 63, 437–441. doi:10.1177/1071181319631016.

Oates, B., 2006. Researching Information Systems and Computing. Researching Information Systems and Computing, SAGE Publications. URL: https://books.google.no/books?id=ztrj8aph-4sC.

Oosthoek, K., Doerr, C., 2021. Cyber threat intelligence: A product without a process? International Journal of Intelligence and CounterIntelligence 34, 300–315. URL: https://doi.org/10.1080/08850607.2020.1780062.

Oyewole, T., 2016. Application of situation awareness in incident response. ISACA Journal URL: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/application-of-situation-awareness-in-incident-response.

Paré, G., Trudel, M.C., Jaana, M., Kitsiou, S., 2015. Synthesizing information systems knowledge: A typology of literature reviews. Information Management 52, 183–199. URL: https://www.sciencedirect.com/science/article/pii/S0378720614001116, doi:https://doi.org/10.1016/j.im.2014.08.008.

Patticrew, M., Roberts, H., 2006. Systematic reviews in the social sciences: A practical guide URL: https://books.google.no/books?hl=en&lr=&id=ZwZ1_xU3E80C&oi=fnd&pg=PR5&ots=wZR2AOKWOp&sig=qEPUuk93ehz_n1oCfH_N4mNkDdg&redir_esc=y#v=onepage&q&f=false.

Podzins, O., Romanovs, A., 2019. Why siem is irreplaceable in a secure it environment? , 1–5URL: https://ieeexplore.ieee.org/abstract/document/8732173/citations#citations, doi:10.1109/eStream.2019.8732173.

Rajivan, P., Cooke, N., 2017. Impact of Team Collaboration on Cybersecurity Situational Awareness. Springer International Publishing, Cham. pp. 203–226. URL: https://doi.org/10.1007/978-3-319-61152-5_8, doi:10.1007/978-3-319-61152-5_8.

Sarker, S., Xiao, X., Beaulieu, T., Lee, A.S., 2018. Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). Journal of the Association for Information Systems 19(8), 752–774. doi:https://doi.org/10.17705/1jais.00508.

Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R., 2017. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives URL: https://aisel.aisnet.org/wi2017/track08/paper/3/?ref=https://githubhelp.com.

Skopik, F., Settani, G., Fiedler, R., 2016. A problem shared is a problem halved. Comput. Secur. 60. URL: https://doi.org/10.1016/j.cose.2016.04.003.

Ursillo, S., Arnold, C., 2019. Cybersecurity is critical for all organizations – large and small URL: https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small.

van der Kleij, R., Schraagen, J.M., Cadet, B., Young, H., 2022. Developing decision support for cybersecurity threat and incident managers. Computers and Security 113, 102535. URL: https://www.sciencedirect.com/science/article/pii/S016740482100359X, doi:https://doi.org/10.1016/j.cose.2021.102535.

Verizon, 2022. 2021 data breach investigations report. URL: https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security operations center: A systematic study and open challenges. IEEE Access 8, 227756–227779. URL: https://ieeexplore.ieee.org/document/9296846, doi:10.1109/ACCESS.2020.3045514.

Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E., 2019. Cyber threat intelligence sharing: Survey and research directions. Computers and Security 87, 101589. URL: https://www.sciencedirect.com/science/article/pii/S016740481830467X, doi:https://doi.org/10.1016/j.cose.2019.101589.

Walsham, G., 1993. Interpreting Information Systems in Organizations. doi:https://doi.org/10.1177/017084069401500614.

Xiao, Y., Watson, M., 2019. Guidance on conducting a systematic literature review. Journal of Planning Education and Research 39, 93–112. URL: https://doi.org/10.1177/0739456X17723971, doi:10.1177/0739456X17723971, arXiv:https://doi.org/10.1177/0739456X17723971.

Yin, R.K., 2014. Case Study Research: Design and Methods. URL: https://www.akademika.no/case-study-research-design-and-methods/yin-robert-k/9781483322247r180.