jamk

Cybersecurity situational awareness in public sector organizations

Design research of a cybersecurity situational awareness model

Juha Jämsen

Master's thesis
August 2024
Master's Degree Programme in Information Technology, Cyber security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Jämsen, Juha

Cybersecurity situational awareness in public sector organizations, Design research of a cybersecurity situational awareness model

Jyväskylä: Jamk University of Applied Sciences, August 2024, 128 pages.

Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

The state of the cyber environment has significantly evolved in recent years within public administration and critical infrastructure organizations of Finland, highlighting the importance of understanding the current state and predictability of the cyber environment. The study focuses on cybersecurity situational awareness (CSA) in public sector organizations, aiming to enhance resilience through a practical model developed. The study involved a theoretical groundwork to identify key CSA components and processes and empirical research with semi-structured interviews from various public sector representatives. These interviews provided insights into current CSA practices, challenges, and needs, leading to the development of a CSA model.

The findings revealed a common three-tiered model of situational awareness—operational, tactical, and strategic—widely used in the public sector. The research emphasized the necessity of inter-organizational cooperation and information sharing for comprehensive situational awareness. It also highlighted the lack of systematic data collection, integration, and analysis processes, causing information silos, manual work and delayed decision-making.

The study proposed a tailored CSA model for public sector organizations, including processes for data collection, integration, analysis, visualization, and decision-making, with a focus on continuous improvement and feedback. The model outlines technological capabilities and sources for CSA and visualizes cooperation and information sharing.

The conclusions stress the need for a structured and systematic CSA approach, combining technological solutions with collaboration, data sharing, and continuous improvement processes. The study offers recommendations for adopting standardized CSA processes, establishing regular inter-organizational collaboration mechanisms at the national level, and implementing advanced data analysis and visualization tools.

Keywords/tags (subjects)

Cybersecurity, situational awareness, threat intelligence, public sector information security, cybersecurity cooperation

Miscellaneous (Confidential information)

-

Contents

Figures

1 Introduction

In the rapidly evolving landscape of cybersecurity, the importance of situational awareness in the public sector cannot be overstated. This master's thesis addresses a critical issue in cybersecurity: the development and implementation of effective cybersecurity situational awareness models for public sector organizations. The research is driven by the increasing complexity and frequency of cyber threats, which necessitate robust mechanisms for understanding, monitoring, and responding to cyber incidents.

The primary issue tackled by this research is the formation and enhancement of cybersecurity situational awareness (CSA) within public sector organizations. Cybersecurity situational awareness refers to the ability to perceive, understand, and predict cybersecurity events to make informed decisions. In the context of public sector organizations, which often handle sensitive information and critical infrastructure, the stakes are particularly high. The research identifies several key challenges: dealing with information overload, ensuring timeliness and accuracy of data, fostering inter-organizational cooperation, and understanding the decision-making processes influenced by situational awareness.

This research serves the urgent need to develop a comprehensive and practical model for cybersecurity situational awareness tailored to the specific requirements of public sector organizations. The proposed model aims to enhance the ability of these organizations to anticipate and respond to cybersecurity threats, improve the integration and analysis of cybersecurity data from multiple sources, foster better cooperation and information sharing among public sector entities and between the public and private sectors, and provide a structured framework for decision-making processes based on situational awareness information.

The goals of the research were multifaceted. Firstly, it sought to define cybersecurity situational awareness by establishing a clear understanding of its components and significance. Additionally, the research aimed to identify current practices and challenges through a combination of theoretical review and empirical research, including interviews with public sector organizations. Based on the insights gained, the next goal was to develop a model that could be implemented across various public sector organizations to enhance their cybersecurity posture. Finally, the research aimed

to provide actionable recommendations for public sector organizations to improve their cybersecurity situational awareness and response strategies.

To systematically address these goals and tasks, the research methodology involved several key phases. The initial phase was a comprehensive literature review to understand existing theories and models of cybersecurity situational awareness. This review covered processes for forming situational awareness, methods for data collection and analysis, visualization techniques, and decision-making processes. The next phase involved empirical research through semi-structured thematic interviews with representatives from various public sector organizations. These interviews aimed to gather practical insights into current practices, challenges, and needs related to cybersecurity situational awareness. The interview data was then transcribed and analyzed to identify common themes, challenges, and best practices, which informed the development of the proposed CSA model.

The model was developed based on both theoretical and empirical findings, incorporating processes for direction, data collection, integration, analysis, visualization, and decision-making. The model describes the technical capabilities and information sources of CSA, the necessary process steps and insight of cooperation mechanisms. As a part of the developed model, a proposal was made for the content of cybersecurity situational picture in different levels and what kind of decision is made in these organizational levels. The research provided a set of recommendations for public sector organizations to implement the proposed CSA model effectively, aimed at enhancing their cybersecurity posture and improving their ability to respond to cyber threats.

In conclusion, this master's thesis addresses a critical gap in the field of cybersecurity by developing a practical and comprehensive model for situational awareness tailored to the needs of public sector organizations. The research highlights the importance of integrating diverse data sources, improving inter-organizational cooperation, and enhancing decision-making processes to respond effectively to cyber threats. The proposed model and recommendations provide a valuable framework for public sector organizations to improve their cybersecurity situational awareness and resilience in the face of evolving cyber threats.

2 Description of the research

2.1 Research topic

The topic of the study was to investigate and evaluate how the cyber security situational awareness and situational picture are formed, what kind of information exchange and cooperation are involved in forming the situational awareness, and what are the key challenges related to forming the situational awareness. By the theoretical review, the aim was to form an understanding of what is generally meant by the term cyber security situational awareness based on various sources, what the process of forming cyber security situational awareness is, what methods are used to collect information for situational awareness, how its visualization and presentation can be done, and what kind of decision-making is associated with situational awareness. The aim of the interviews in the study was to find practical experiences of how situational awareness is currently formed in public administration organizations or organizations providing ICT services to them, how situational awareness is used to support decision-making and how methods of situational awareness should be developed in public sector. In the interviews, one aspect was to find out how different organizations exchange information related to situational awareness within the industry, at the national and international levels. Identifying the current challenges and issues and finding perspectives on how situational awareness formation can be developed in public administration organizations was one key targets for the interviews.

Based on the theoretical review and the results of the interviews, a model was developed that can be utilized for forming cyber security situational awareness across different industries. The interview questionnaire is also designed in a way that its responses support the creation of the developed situational awareness model. In designing the model, the following questions are taken into consideration:

- What does cybersecurity situational awareness as a term means?
- What are the levels of forming situational awareness and picture?
- What kind of processes existed for situational awareness?
- How are situational awareness and picture directed?
- What are the data areas and sources of situational awareness and picture?
- How is the data collected from internal and external cyber environment?

- How is situational awareness data processed and composed?
- How is the threat intelligence executed?
- What kind of co-operation and information sharing is needed for situational awareness?
- How is the situational picture presented and visualized?
- What kind of decisions are made based on situational picture?
- How are the decisions effectiveness measured?

The topic was considered timely because according to the National cyber security center's Year 2022 in cybersecurity -report, Finland's security situation has changed significantly. This change has been influenced by factors such as Russia's extensive attack on Ukraine that began in February 2022, the COVID-19 pandemic, and Finland's NATO membership (National Cyber Security Centre, 2023, p. 9).

According to the report, Finnish authorities have issued warnings about extensive hybrid influencing during the year 2022, advising to pay attention to preparing for and responding particularly to cyber-attacks and information influencing (National Cyber Security Centre, 2023, p. 9). Similarly, in the Chief's Review of the Finnish Security Intelligence Service's Yearbook 2023, Teemu Turunen states that Russia's actions pose the greatest threat to Finland's national security. According to Turunen, Russia views Finland as an unfriendly state and directs espionage and broad-based influencing towards Finland, necessitating preparedness for malicious activities in both the short and long term. The Finnish Security Intelligence Service has highlighted heightened threats related particularly to the cyber realm and critical infrastructure in its yearbook (The Finnish Security Intelligence Service, 2024, p. 5). In Finland, recent instances of hybrid influence include a hybrid operation initiated by Russia in 2023, which utilized instrumentalized immigration along Finland's eastern border (Joukanen, 2023). According to the annual report of the Finnish Security Intelligence Service, instrumentalized immigration is also an easy way for Russia to keep Finland on its toes. In addition, several media outlets have reported on Russia's cyber-attacks on critical infrastructure in Western countries, with a recent example being the cyber-attack carried out by Russia on water facilities in Estonia, as reported by Simo Ortamo of Yle news (Ortamo, 2024). According to the Cyber Security Year 2022 report, during the year 2022, ransomware, targeted phishing, and malicious traffic increased in both government agencies and critical infrastructure organizations (National Cyber Security Centre, 2023, p. 9). During the writing of the study, it was also reported in

the media that Helsinki City experienced a data breach, with up to 120,000 individuals' information being stolen, according to Yle News reportes (Jäärni & Rita, 2024). According to various sources, the security situation has changed, and creating cyber situational awareness is one key tool for understanding its impacts within one's own organization. Given that security threats are particularly targeted at government agencies and organizations providing critical services, the interviewees for the study were selected from government agencies and social and healthcare service-producing wellbeing services counties.

The choice of topic was influenced by the challenges encountered in the author's own cybersecurity consulting work regarding the collection and presentation of cyber situational awareness to organizational leadership, as well as the varying perceptions of the purpose of cyber security situational awareness. The research novelty lies in the fact that the formation of cyber security situational awareness has been relatively underexplored at the public sector level and based on the results of the literature review process, comprehensive frameworks specifically targeting cyber security situational awareness of public sector are scarce beyond individual processes. The study also provides a current state insight of the maturity of situational awareness formation in the interviewed organizations and presents areas for improvement in developing situational awareness capabilities. This brings societal value to the research.

2.2 Research questions

Given the research topic, the research questions are formulated to address the identified research problem. The research problem is that the concept of cyber security situational awareness is understood differently in different organizations, leading to its implementation through varying methods and at different organizational levels. Particularly, there is scarce existing research on the formation of cyber situational awareness in wellbeing services counties from public sources. This is also influenced by the fact that wellbeing services counties have been established since 2023. Based on the conducted literature review, only a few ready-made frameworks or models are found for the formation of cyber security situational awareness. Instead, existing publications often focus on the general process of situational awareness or on specific areas of cyber situational awareness, such as improving cybersecurity monitoring, threat intelligence, and incident detection. In existing models, the specific phases are also not explicitly described, possibly because they are intended to be broadly applicable. The research questions aim to find concrete answers and

thus clarify the understanding of the purpose and significance of cyber security situational awareness, leading to the creation of a widely applicable practical model for building cyber security situational awareness. Practical insights into the research problem are sought from government agencies and wellbeing services counties that provide critical services to society, thereby considered to have a high level of preparedness. The main research questions are as follows:

1. How is cyber security situational awareness formed in public sector organizations, and what are its key areas for improvement?
2. How is cyber security situational awareness utilized in decision-making processes within public sector organizations?
3. What kind of cooperation and information sharing is needed to form a comprehensive cyber security situational awareness?

The research questions support the goal of the study to form a general model for creating a cybersecurity situational awareness in organizations. By answering how situational awareness is currently formed in different organizations, how it is utilized in decision-making, and what kind of collaboration is needed, valuable information was provided to support theoretical knowledge for a generalized model of cybersecurity situational awareness formation.

The starting assumption was that cybersecurity situational awareness is formed variably at different levels within organizations, using a wide range of methods and technologies. It is also assumed that the term "cybersecurity situational awareness" is understood in various ways. Regarding decision-making, the assumption is that situational awareness information is used to react to various operational events, such as security incidents, and to assess their impacts, as well as to evaluate the effects of identified security threats, and what actions should be taken. These actions may include investments, increases in resources, or the initiation of new development projects. Concerning cooperation, the assumption is that within government organizations, there is closer collaboration at the national and international levels, whereas within wellbeing services counties, collaboration primarily involves intra-industry information exchange. These assumptions are based on the author's own experiences in cybersecurity consulting across various client engagements.

2.3 Scope of the research

The thesis was scoped down to focus on the formation of cybersecurity situational awareness, particularly from the perspective of public sector organizations and the companies providing them ICT services. For interviews, representatives from government organizations and wellbeing services counties within the public sector were invited. Regarding the scope, there was consideration given to focusing solely on the current situation and development needs of wellbeing services counties. However, a slightly broader perspective and comparability were desired for the development of the model, which led to the inclusion of other groups within the public sector, government agencies, as well as ICT service providers. The research topic was targeted at the formation of cybersecurity situational awareness, but since cybersecurity is part of an organization's overall security, the interviews also superficially explored what other situational information is reported to different levels of the organization from the perspective of overall security. The formation of cyber situational awareness consists of several different cybersecurity areas, so the topic could have been further refined, but the research intentionally aimed to create a model that covers all the key stages of forming cybersecurity situational awareness. Many other studies have focused on more specific areas of cybersecurity, such as incident management and the derived situational awareness. Figure 1 illustrates the scope of the research.

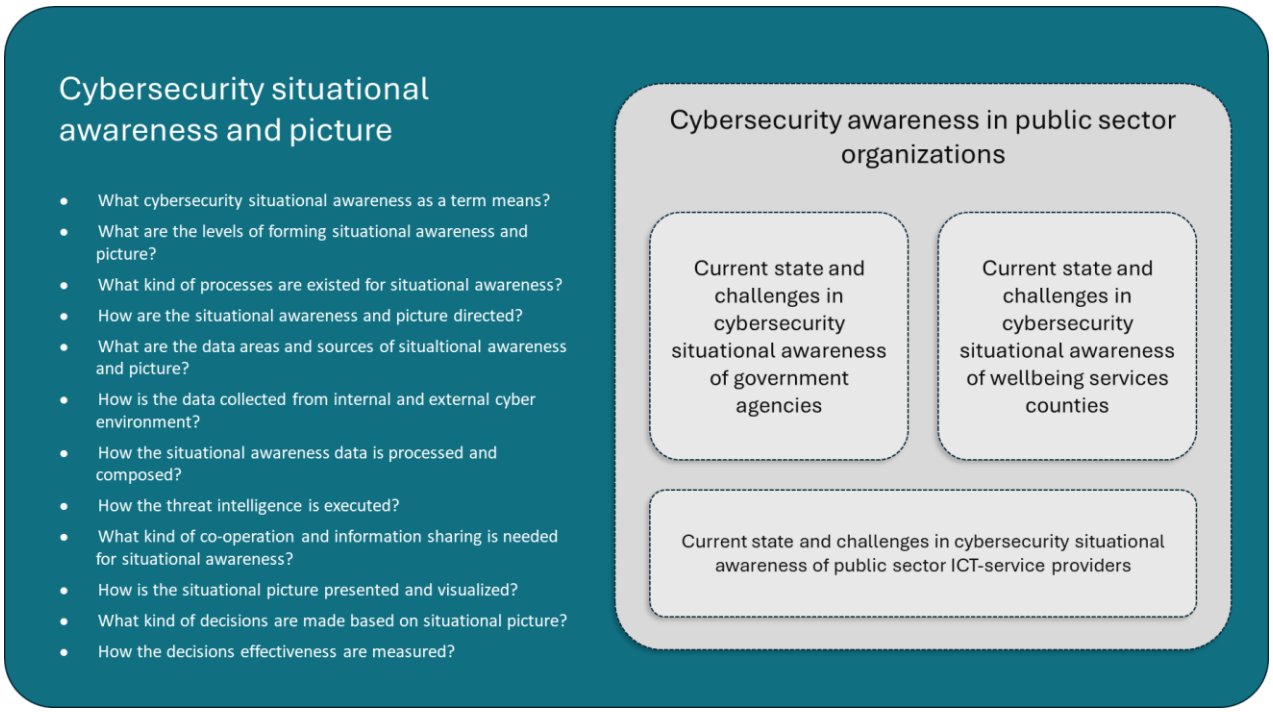

Figure 1 - Scope of the research

Based on the research findings, the model developed for forming cybersecurity situational awareness can also be applied in other sectors beyond the public sector, but it is based on the perspective outlined in the scope. In this study, the situational information base for forming the organization's situational awareness is defined to encompass both internal and external operating environments. The internal operating environment refers to cybersecurity events and phenomena within the organization's internal operations and ICT environments. The external operating environment refers to events and phenomena related to the organization's stakeholders, industry, and for example, national cybersecurity.

2.4 Previous researches

Based on the literature review situational awareness and the process of forming situational information have been studied to some extent in various theses and master's theses from different universities. Additionally, there have been some articles published that investigate, for example, the development of cybersecurity situational awareness among critical infrastructure operators and the strategic management of cybersecurity in public administration. However there are not many studies specifically focusing on cybersecurity situational awareness in public sector organizations. The following are selected excerpts from publications specifically related to this research area.

Mustajärvi, R. (2023). ***Impact of SOC Pilot Implementation on Situational Picture: Analysis and Application to Security Management*****. Centria University of Applied Sciences.** This study focused on the Security Operations Center (SOC) and how SOC functions impact cybersecurity situational awareness. Specifically, the study examined how SOC piloting can improve an organization's responsiveness, identify vulnerabilities, mitigate threats, and enable faster action in critical cybersecurity situations. The outcome of the thesis provided a comprehensive understanding of how SOC piloting can enhance cybersecurity situational awareness, as well as concrete tools for planning and implementing SOC pilot projects (Mustajärvi, 2023, p. 9-10).

Martti L., Jarno L., Tuomas K., Jouni P. & Mirva S. (2018). ***Strategic management of cyber security in Finland.*** **Prime Minister´s Office.** Lehto, Limnéll et al.'s research project aimed to define what strategic leadership in cybersecurity entails and how it is implemented within the framework of comprehensive security responsibility. The objectives included establishing how a general crisis

management model is applied in large-scale cybersecurity incidents, organizing strategic cybersecurity leadership, and determining the structure of cybersecurity management in government institutions. The study also proposed action plans for strategic cybersecurity management in society and public administration, managing extensive disruptions in the cybersecurity environment, and measuring cybersecurity status. Additionally, the research analyzed foreign cybersecurity solutions and situational awareness models. Based on the findings, national cyber capabilities are becoming increasingly crucial for overall security and safeguarding vital societal functions. A clear strategic-level leadership model and a supportive situational awareness are necessary for national development and preparedness, as well as for managing severe and extensive disruptions in cybersecurity environments during both normal and emergency situations (Lehto, Limnéll et al., 2018, p. 2).

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J. (2019). ***Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations*****. Information & Security: An International Journal 43:2, 236-256.** This study investigated how the cyber situational awareness of critical infrastructure organizations can be enhanced, how these organizations exchange cybersecurity-related information, and whether the organization's cybersecurity capabilities can be utilized more broadly. According to the research, good situational awareness and information sharing among groups with different interests have a significant impact on managing cyber disruptions. The research method employed open-ended theme interviews with material-based content analysis. A total of 40 individuals from 25 private or public organizations, who were either leaders or individuals responsible for information/cybersecurity within their organizations, were interviewed. The study included three sub-areas of critical infrastructure: services, telecommunications networks, and power grids (Pöyhönen, Nuojua et al., 2019).

Hedeman E., (2022), ***Cyber Situational Awareness at the Prime Minister's Office*****. Laurea University of Applied Sciences**. Elina's thesis aimed to create an administrative-level process for the Prime Minister's Office (VNK) that encompasses the production and utilization of a cybersecurity situational awareness. The development problem was that the Prime Minister's Office did not systematically produce a cybersecurity situational awareness from its own organizational perspective. The outcome of the thesis was a proposed process for situational awareness formation for the Prime Minister's Office (Hedeman, 2022).

Salomaa, J. (2019), ***Measuring and Creating Situational Awareness in Cybersecurity: The Requirements Specification for Situational Awareness and Metrics Platform*****. South-Eastern Finland university of applied sciences.** Salomaa's master's thesis aimed to explore the key elements and relevance of cybersecurity metrics. Additionally, the research focused on the general requirements of cybersecurity metrics platforms, how the measured information is visualized, and what are the essential data sources for creating cybersecurity situational awareness. The objective of this study was to identify and define the relevant requirements for cybersecurity metrics and situational awareness platforms. The main outcome of the thesis was the collected examples of cybersecurity metrics and the requirements for the cybersecurity situational awareness platform (Salomaa, 2019).

Teriö, J. (2017). ***Toward cyber situational awareness with open source software*****. University of Jyväskylä.** This study aims to describe how cybersecurity situational awareness can be achieved using open-source software. It outlines the necessary elements, data collection, analysis, and visualization, as well as the benefits of cybersecurity situational awareness for decision-makers. The study employs the design science research method to design and build a solution, demonstrating its suitability for creating cybersecurity situational awareness. The result is a system that uses open-source software to establish situational awareness, consisting of a management server and two client servers. The study produces a description of utilizing open-source software in building cybersecurity situational awareness (Teriö, 2017).

3 Research methods

The aim of the research was to develop a model for forming a cyber security situation picture based on theoretical knowledge and conclusions drawn from interviews. The research methodology initially involved semi-structured thematic interviews. According to Hirsijärvi & Hurme (2011), in a semi-structured thematic interview, each interview is focused on a specific theme, with the questions being the same for all participants. However, the interviewer has the flexibility to change the order of the questions, and the questions are not tied to predefined answer options. Instead, the interviewees are free to respond to the questions in their own words (Hirsijärvi & Hurme, 2011, p. 47). The chosen semi-structured thematic interview method would be suitable for understanding the current state and development goals of the target organizations if the goal was solely to gather information. The purpose of the interviews was to collect data from real public administration organizations without predefined answer options, but with the same set of questions for all participants, making it easier to draw conclusions. However, since the emphasis of the work was on developing a model for cyber security situation awareness, a qualitative developmental research method was more suitable. In this approach, interviews were one of the data collection methods used.

According to Kananen (2012), development work is typically motivated by a phenomenon, process, or state of affairs that is desired to be improved after the development or change. Developmental research often involves the adaptation or application of an existing solution to a different operating environment (Kananen, 2012, p. 19). In this study, the development process can be considered as the general process of forming a situational picture, to which concrete elements from the perspective of cybersecurity are developed based on the theoretical knowledge and practical experiences gathered in the research. The study also delved into the processes related to cyber threat intelligence, the features of which are taken into account in the developed model.

The thesis was originally written in Finnish but was translated into English in the final stages of the work, utilizing artificial intelligence. ChatGPT was used as the translation tool for written theory part text, and the resulting text was reviewed to ensure it closely matched the original Finnish text.

3.1 Research structure

The structure of the research is designed so that its phases systematically support each other, ensuring that there is existing background information for each stage of the research. According to Kananen (2012), writing a development research thesis follows the same pattern regardless of whether it is a qualitative or quantitative action or development research (Kananen, 2012, p. 13). In the first phase of the study, the research objectives and questions are defined based on the identified research problem. In addition to the research questions and objectives, the first phase of the work includes the introduction of solution tools and approaches, which involve reviewing theoretical knowledge and conducting interviews, along with related data collection methods. In the second phase, conducted in the theoretical literature review, the term and concept of cyber security situation awareness are first described to establish an understanding of what the concept generally entails and how it is delineated. Following this, the theoretical section delves into the process of forming cyber security situation awareness, its stages, and methods. The literature review investigates, among other things, the basis for collecting and reporting situation awareness data, as well as the type of information gathered for the situation awareness. The theoretical section also examines how the cyber security threat intelligence is formed, how threats in the organization's internal and external operating environment are identified and analyzed, how they are incorporated into the situation awareness, and what decision-making processes are involved.

After the theoretical section, in phase three, the planned interview work is conducted with selected public administration target organizations. The formulation of interview questions has been informed by theoretical knowledge and is based on the research objectives and main questions. The interviews were transcribed, and a summary was derived from them.

Based on the results of the interviews, an analysis was conducted to identify elements and clarifications from real-life scenarios for forming and improving the situational awareness. In the fifth phase, a cyber security situational awareness model consistent with the objectives was formulated and described. The final stage of the research involved summarizing the research work and presenting possible identified areas for further research. Figure 2 visualizes the structure and phasing of the research work, according to which the table of contents is also structured.

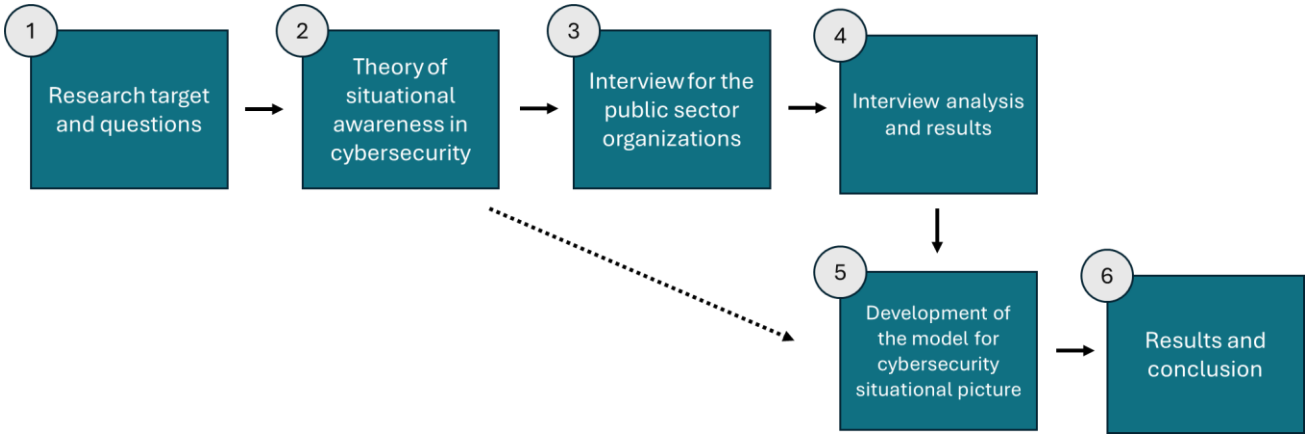

Figure 2 - Structure of the research

3.2 Data acquisition methods

Figure 3 illustrates the methods of data collection used in the study. The first method employed for data collection involved identifying existing research publications, which were gathered into the theoretical framework of the study using various search engines. From these, the most relevant sources were selected for the study.

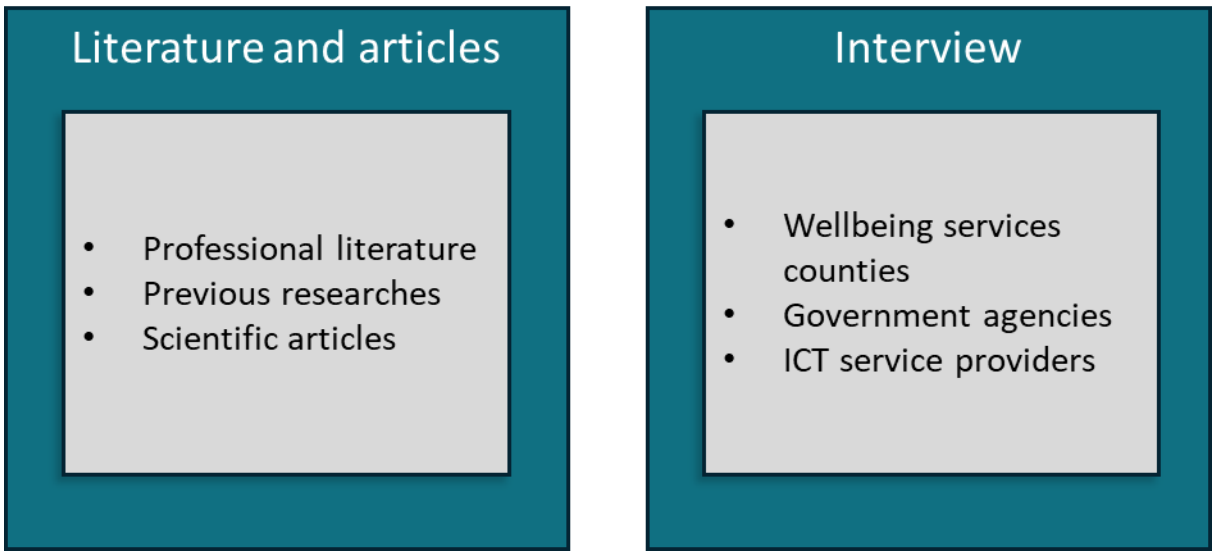

Figure 3 - Data acquisition methods

Based on the theoretical knowledge, the aim was to understand what is meant by cyber situational awareness and how it can be formed, how cyber threat intelligence supports the formation

of cyber situational awareness, how collaboration can be implemented in terms of cyber situational awareness, and how the current state and desired state of cyber situational awareness in the Finnish public administration are based on theoretical knowledge. Figure 4 illustrates the stages of forming the theoretical foundation.

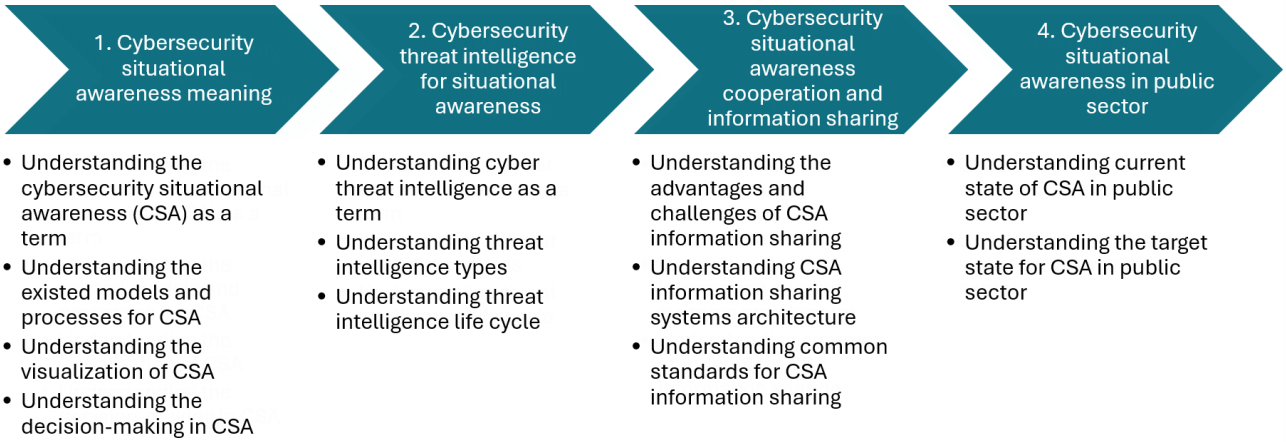

Figure 4 - Literature review process for the research

The second central method was to gather information about the current state of existing organizations by conducting interviews. Interviews were arranged with organizations from the central government and well-being regions, as well as companies providing ICT services to them. Interviews were scheduled by directly contacting the responsible parties for cybersecurity or business operations in these organizations.

3.2.1 Literature and articles

The material related to cyber situational awareness was collected and searched for from various sources, primarily over the past 10 years from 2014 to 2024. For some themes, older sources had to be used, especially in cases where a general model had been developed long ago but is still used today for situational awareness. The main search engines used for collecting the material were Google Scholar and the Janet database of educational institutions' libraries. Several keywords or phrases were used in the searches. The following search phrases led to the key publications utilized in the study:

- ”Cyber security situational awareness”

- ”Cyber security situational picture”
- ”Situational picture”
- ”Situation picture process”
- ”Threat intelligence”
- ”Cyber threat intelligence”
- ”Cybersecurity reporting”
- ”Cybersecurity situational awareness process”
- ”Cybersecurity management decisions”
- ”Cybersecurity information sharing”
- ”Cybersecurity collaboration”
- ”Decision-making in cybersecurity”
- ”Kyberturvallisuus tilannekuva suomessa”
- ”Kyberturvallisuus sosiaali- ja terveysalalla”
- ”Kyberturvallisuus valtiohallinnossa”
- ”Data gathering process”

The search results yielded articles and previous studies specifically targeting situational awareness, but some of the sources had to be excluded due to their old publication dates. Additionally, sources for the study were found by reviewing previous research. From the articles utilized in the study, additional sources relevant to this research were identified. Overall, data collection was somewhat challenging because there haven't been many targeted studies specifically on the topic of cyber situational awareness in public sector organizations. Instead, cyber situational awareness is often a component of broader research or, for example, a section of a standard. The following describes the search results and sources for the theoretical framework of the research by topic.

Description of the research and research methods

- Amount of sources was good, over ten found, chosen for the research 12 references

- Lots of information can be found about existed cyberattacks and breaches. Also, multiple cyber treat landscape reports can be found on the internet. Multiple books and other literature about planning and execution of thesis work based on interview and design research approaches.

Cybersecurity situational awareness:

- Total amount of search results in Janet was 33 141 with the search phrase “Cyber security situational awareness”
- Amount of relevant sources was good, multiple dozens found, chosen for the research 17 references
- Focused mostly on Endsley’s model of situational awareness, including some adaptations existed for SA in cybersecurity context.

Cyber threat intelligence for situational awareness:

- Total amount of search results in Janet was 361 311 with the search phrase “Cyber threat intelligence”
- Amount of relevant sources was decent, over ten found, chosen for the research 5 references
- Most of the cyber threat intelligence models and processes are based on common intelligence cycle of military sector

Cybersecurity situational awareness cooperation and information sharing:

- Total amount of search results in Janet was 2 189 with the search phrase “Cybersecurity situational awareness cooperation and information sharing”
- Amount of relevant sources was decent, over ten found, chosen for the research 5 references
- Some researches done by Finnish institutions, some international researches
- Some standardization existed for threat information sharing

Cybersecurity situational awareness in Finland's public sector:

- Total amount of search results in Janet was 438 with the search phrase "Cybersecurity situational awareness in Finland's public sector"
- Amount of relevant sources was poor, was less than ten found, chosen for the research 6
- Most of the sources are based on some Finnish public sector organization's researches and reports, only few scientifical research articles.

As a result of the searching literature and articles related to the theme of the research, totally 45 references were chosen. Mainly these references were other studies and articles of some scientific journals including some publication of Finnish government agencies and other organizations reports.

3.2.2 Interviewed organizations

The research was limited to public administration organizations. According to the Ministry of Finance's website, Finland's administrative structure consists of the highest elected bodies, which are Parliament, the President of the Republic and the Government, and of independent courts of law, state administration and other public administration. Other public administration entities include municipalities and wellbeing services counties (The Ministry of Finance). Due to the scope of the study, two groups of organizations within the public administration were selected: wellbeing services counties and government agencies. The selection was influenced by the fact that organizations within these groups are often relatively large and provide important digital services to citizens and businesses. It can be assumed that they are also more likely to face cyber threats compared for example to smaller municipal actors. Additionally, the study aimed to include companies providing ICT services to these organizations, especially those with ownership ties to the mentioned entities.

The interviewees were selected from public administration organizations from wellbeing services counties, government agencies, and companies providing ICT services to them. There was a total of eight organizations interviewed, consisting of four wellbeing services counties, two government

agencies, and two ICT service providers. The organizations were approached by sending them inquiries about their interest and willingness to participate in the study. Along with the invitations, presentation material about the research was provided to all potential interviewees. The highest interest was observed from the wellbeing services counties, resulting in more participants from this group compared to others. In total, there were 11 individuals interviewed. The interviewed group and the number of participants is illustrated in Figure 5. The interviewees held positions such as responsible for information security, information security experts, or heads of information security business. It was considered that this group of experts would have the best insight into the formation and reporting of cyber security situation awareness at both managerial and operational levels.

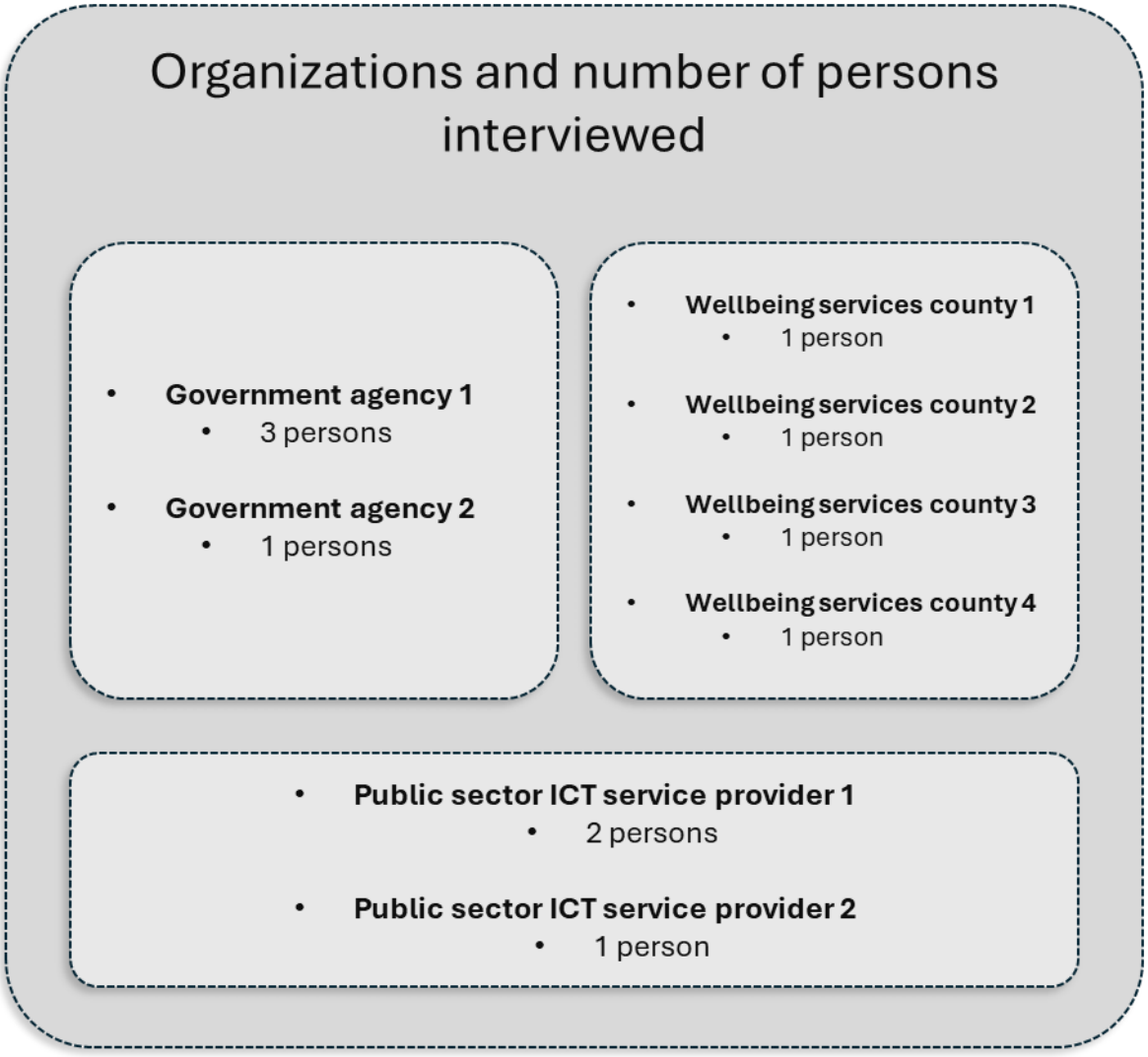

Figure 5 - Organizations and number of persons interviewed

3.2.3 Execution of the interview

The interview was conducted using the Microsoft Teams application, and the interview discussions were recorded and transcribed. As a principle, the organizations and individuals interviewed were not mentioned by name in the research report to ensure their anonymity. The responses were kept anonymous because they might reveal weaknesses or other sensitive information about the organization, which could potentially be exploited by outsiders, such as in cyberattacks. Publishing the names of the organizations or interviewees could have reduced the willingness to participate in the study. The duration of the interview was set to one hour, as indicated in the invitation. The structure of the interview consisted of the following main points.

- Introductions, about 5 minutes
- Brief introduction to the study, including an explanation of the term "cybersecurity situational awareness" based on theoretical knowledge, about 5 minutes
- Presentation of interview questions and answers, about 45 minutes
- Possible follow-up actions and conclusion of the interview, about 5 minutes

Before the actual interview, a separate briefing lasting about half an hour was held with some interviewees to go through the purpose of the study, and at the same time, a more precise time for the actual interview was agreed upon.

After the interview, the transcriptions of the discussions were compiled into a single Excel spreadsheet, where the answers were categorized question by question into their own rows and columns. Based on this, a summary of the interview results was created.

3.2.4 Interview questions

The interview questions were designed to support the main research questions of the study and the goal of creating a general model for forming cybersecurity situational awareness. The aim of the interview was to seek organizations' views on how cybersecurity situational awareness is understood in their organizations, how it is currently implemented, and what identified challenges and development measures exist. The number of questions was planned to provide a sufficient

picture of the organization's perspectives on the research questions, considering the available time. There was a total of 15 questions, which are listed below. Along with the questions, the interviewees were informed about the purpose of the interview and the Security Committee's tacit definition of cybersecurity situational awareness.

1. **Target Groups for Cybersecurity Situational Awareness:** At what different levels is cybersecurity situational awareness formed in your organization, and to whom is it reported (e.g., tactical, operational, or strategic levels)?

2. **Reporting Cycle**: How often is cybersecurity situational awareness reported in your organization at different levels?

3. **Process of Cybersecurity Situational Awareness Formation:** Do you utilize any specific documented model, method, or process in forming the situational awareness and picture?

4. **Steering of Cybersecurity Situational Awareness:** How is the collection and production of situational awareness data steered in your organization?

5. **Data Collection and Coverage for Cybersecurity Situational Awareness:** What type of information or data areas does your cybersecurity situational awareness consist of?
    a. Regarding the internal operating environment?
    b. Regarding the external operating environment?

6. **Observation and Data Collection for Cybersecurity Situational Awareness:** What methods or technologies do you use to gather data for the cybersecurity situational awareness?

7. **Data Integration, Analysis, and Reporting:** How do you refine and generate analyses, reports, or possible conclusions from the collected data to support decision-making?

8. **Visualization of Cybersecurity Situational Awareness:** How do you visualize your cybersecurity situational awareness in understandable forms at different levels (e.g., tactical, operational, or strategic levels)?

9. **Decision-Making:** What cybersecurity-related decisions are made in your organization at different levels or their groups based on the situational awareness data?

10. **Measurement of Decision Impact:** Do you monitor or measure the impact and implementation of decisions based on situational awareness?

11. **Cooperation for Cybersecurity Situational Awareness:** Do you share your situational awareness information with your stakeholders or partners, and through what methods?

12. **Cooperation for Cybersecurity Situational Awareness:** Do you utilize situational awareness information produced by others in forming your own situational awareness?

13. **Cooperation for Cybersecurity Situational Awareness:** What other cooperation related to cybersecurity situational awareness do you engage in with different stakeholders, for example, sector-specific, national, or international levels?

14. **Challenges of Cybersecurity Situational Awareness:** What are the key challenges, problems, and development needs in forming and utilizing your cybersecurity situational awareness, and how could these be addressed or the current situation improved? (e.g., regarding processes, technologies, resources, collaboration)

15. **Cybersecurity Situational Awareness as Part of Overall Security:** Do you also form a situational awareness of other security issues in your organization, such as the overall security situation, where cybersecurity is one part of the whole?

4 Cybersecurity situational awareness

4.1 Situational awareness in cybersecurity

One central aspect of the research problem was understanding and describing the term "cybersecurity situational awareness." The concept of situational awareness has been discussed in various publications, often with reference to Endsley's description. According to Endsley, Lieutenant Colonel Mike Press traced the role of situational awareness in the aviation environment back to World War I flying ace Oswald Boelcke in 1986 (Endsley, 1990, p. 5). In the early years of flying, Boelcke learned the importance of gaining awareness of the enemy before the enemy became aware of him and thus developed methods to achieve this (Endsley, 1990, p. 5). Endsley (1990) says, situational awareness refers to the activity of gathering information and creating an understanding of what is happening and predicting what will happen in the near future. Endsley (1990) states in her dissertation that situational awareness can be thought of as a pilot's internal model of the surrounding world at any given time. The pilot's ability to maintain situational awareness has long been recognized in the aviation community as a key factor in mission success and survival (Endsley, 1990, p. 5).

According to Pöyhönen, Rajamäki et al. (2021), the prerequisite for an organization's operation is to obtain information about its environment and events, as well as their impact on its operations. Proper and timely situational awareness relies on accurate information and assessments, and it becomes crucial in cases where broad decisions must be made on a tight schedule. To make the right decisions, decision-makers must understand the basis of their decisions, their implications, how others will react to them, and the risks associated with them. Therefore, decision-makers need to have sufficient situational awareness and understand all operational levels, enabling timely decision-making and action. Pöyhönen, Rajamäki et al. (2021) says that situational awareness generally refers to a description prepared by experts of the prevailing conditions and the operational capabilities of various actors, events caused by disruptions, their background information, and assessments of the situation's development. In addition, situational awareness can include operational recommendations based on data analysis (Pöyhönen, Rajamäki et al., 2021, p. 3).

Kokkonen (2016) writes in his article that Cyber Security Situational Awareness System means that there is multi sensor information available indicating what is happening, there is the capability for analyzing such information, and there is also capability for making predictions what will happen in the near future. Kokkonen (2016) says that there are three types of information needed for situational awareness in cyber security. The types are information of computing and network components, threat information, and information of mission dependencies (Kokkonen, 2016, s. 2).

The term "situation awareness" is defined in the Security Committee's comprehensive security glossary as follows, *"A compiled description of prevailing conditions, events leading to the current situation, background information about the situation, assessments of the situation's development, and the operational readiness of various actors."*. According to the glossary, situational awareness is needed to support decision-making, and situational awareness can also be understood more narrowly to refer only to, for example, a map and oral or written information about the current situation. Based on the definition, the term "situation picture" is used to refer to a concrete description of the situational awareness. However, if the term "situation picture" also refers to situational activity or the state in which a situation has been formed, the term "situation awareness" can be used. The glossary states that situational awareness refers to the understanding needed by decision-makers and their assistants for decision-making, including comprehension of events, the conditions that influenced them, the objectives of different parties, and the potential development options of events (Security Committee, 2017, p.64).

According to the cybersecurity glossary published by the Security Committee in 2018, the term "Cyber security situation awareness" refers to a compiled description of the current availability and security situation of information systems at a certain moment, as well as the prevailing state of the cyber operating environment. The glossary notes that cyber security situation awareness is produced to support decision-making and is based on observations, assessments, metrics, and analyses. It also states that cyber security situation awareness can be examined at tactical, operational, or strategic levels and is often produced collaboratively among various stakeholders (Security Committee, 2018, p. 22). The definition from the cybersecurity glossary implies that building cyber security situation awareness involves strong collaboration and that it focuses on the security situation of information systems and cyber operating environments. Additionally, the glossary

mentions that the National Cyber Security Center gathers and coordinates the national cyber security situation awareness (Security Committee, 2018, p. 22). It is good to note that in this study we describe other research of cybersecurity situational awareness where this term is used in different formats and abbreviations, that includes “Cyber Security Situational Awareness (CSSA)”, “Cyber Situational Awareness (CSA)” and “Cyber Common Operational Picture (CyCOP and CCOP)”. In the end all these formats means that same ideology in formation situational awareness in cybersecurity context.

According to the cybersecurity glossary of the Security Committee (2018), the “Cyber operating environment” term refers to an operational environment formed by one or more digital information systems. The cyber operating environment is characterized by the use of electronics and the electromagnetic spectrum for storing, manipulating, and transmitting data and information via communication networks. The environment also includes physical structures related to the processing of data and information. Examples of cyber operating environments include the control systems of nuclear power plants, food transportation and logistics systems, traffic control systems, as well as banking and payment systems (Security Committee, 2018, p. 21).

As the research focuses on cyber security situation awareness, aimed at understanding the prevailing cyber operational environment security situation, it is also essential to understand the purpose of the cyber threat concept. Based on the Security Committee's cybersecurity glossary (2018), a “Cyber threat” term refers to a potentially harmful event or trend that targets the cyber operational environment and, if realized, jeopardizes a dependent function therein. Cyber threats can arise not only from actual cybersecurity threats but also from actions in the digital communication environment that jeopardize societal security. Cyber threats can target vital societal functions, national critical infrastructure, or citizens directly or indirectly. They may originate from within or outside the country's borders. Examples of functions dependent on the cyber operational environment include nuclear power plant control, food transportation and logistics, and traffic control (Security Committee, 2018, p. 25). From the definition of the cyber threat term, it can be inferred that cyber threats to an individual organization can originate not only from internal information system environments but also from external factors, such as events and phenomena affecting society or critical infrastructure. Consequently, cybersecurity situation awareness

can be seen as encompassing both the internal and external operating environment of an organization.

Lehto, Limnéll et al. (2018) describe in their publication that situational awareness is a presentation of the situation or capabilities compiled from selected individual pieces of information, providing the basis for situational understanding. Similarly, situational understanding is the comprehension of events, circumstances influencing them, goals of various parties, and potential developments of events, which are necessary for decision-making on a specific matter or issue. According to Lehto, Limnéll et al. (2018), situational awareness is twofold. Firstly, it is a real-time depiction of the prevailing events concerning security conditions. Information required for situational awareness is gathered from observation systems, public sources, and the organization's own data sources. Secondly, situational awareness includes an analysis of the current situation and an assessment of future events. Situational awareness provides a comprehensive understanding of what has happened, is happening, or will happen. (Lehto, Limnéll et al., 2018, p. 38-40).

Lehto, Limnéll et al. (2018) state that situational awareness can take the form of periodic general assessments or more detailed analyses of current topics or issues, evaluating events and their impacts. Such descriptive, strategic situational awareness can be provided to decision-makers at regular intervals, for example, three times a year, once a month, or once a week. Situational awareness can also be a more frequent, daily overview or event compilation available to actors in the system. In this case, it usually does not include assessments of situation development or recommendations for action (Lehto, Limnnéll et al., 2018, p. 38-40).

Operational-level situational awareness is formed and updated as close to real-time as possible during a disruptive situation. Lehto, Limnéll et al. (2018) notes that in this case, through continuous monitoring and updating, it should provide an overview of the development of events, thus enabling situation management and the leadership actions required to resolve the situation. Decision-makers must be able to trust that the situational awareness provided to them, with all its details, is reliable and the analyses are prepared with the best possible expertise (Lehto, Limnnéll et al., 2018, p.38-39). Situation awareness and understanding require cooperation and expertise that

enable comprehensive monitoring of the operational environment, analysis and compilation of information, information sharing, identification of research needs, and management of networks. (Lehto, Limnnéll et al., 2018, p. 40)

4.2 Endsley's model for situational awareness

The process or model of situation awareness has often been described in various studies based on Endsley's developed model of situation awareness. In this study, we explore this model and its variations, among other existed models, from the perspective of cybersecurity. Endsley (1995) originally developed the model for the context of military aviation, but it has been widely used for developing situation awareness and planning its process. The model describes, in three levels, how situation awareness is formed through observation and analysis to understand the situation and further predict future events (Endsley, 1995, p. 34-35). Onwubiko (2016) describes a variation of Endsley's model in his article, which includes the fourth level "resolution," originally added by McGuinness & Foy (2000), into the situation awareness processing model (Onwubiko, 2016, p. 3). Figure 6 illustrates Endsley's situation awareness model with included the fourth level of situation awareness processing described in Onwubiko's article.

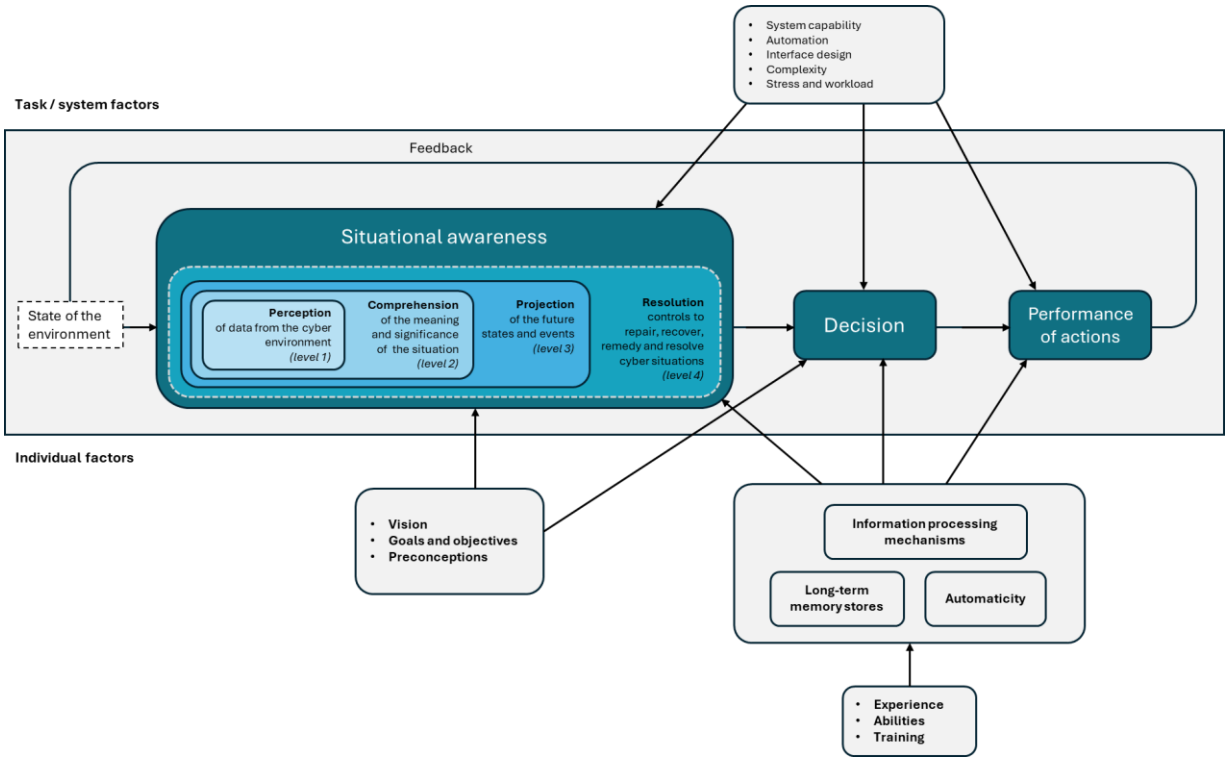

Figure 6 – Endsly's model for situational awareness with extension of McGuinnes & Foy model

4.2.1 Perception

Perception (level 1) involves evidence-based information from sensors about the system and its operational environment. According to Onwubiko (2016) this information may come from surveillance and alarm systems and their sensors, for instance. The data itself can indicate the state of information systems or their components where anomalies or disruptions have been detected. From a cybersecurity perspective, the information comprises raw data reported by firewalls and intrusion detection systems, including source and timestamp information (Onwubiko, 2016, p. 7).

4.2.2 Comprehension

Comprehension (level 2) refers to the precise understanding of the situation derived from the analysis of the information collected about the current state of cybersecurity or observed evidence, including an understanding of the current threat level, types of attacks, and associated risks. Onwubiko (2016) notes that understanding the cybersecurity situation is achieved when analyses are made from the collected data, describing the overall situation of the cyber operational environment and the threats and risks it faces. Based on this information, individuals utilizing the situation picture can understand the vulnerability of the environment or its components and make decisions accordingly (Onwubiko, 2016, p. 7).

4.2.3 Projection

Projection (level 3) describes anticipatory actions to predict future events, situations, or conditions using the current situation and understanding of how current situations could evolve. Onwubiko (2016) notes that it also involves assessing how the current situation could change in the near future, considering the tension, escalations, and developments associated with the current situation that may occur over time (Onwubiko, 2016, p. 7).

4.2.4 Resolution

Resolution (level 4) refers to determining management measures based on the current situation and forecasts of future events to correct, recover, and resolve identified cyber events (Onwubiko,

2016, p. 7). Based on Yasseri (2012) this level aims to pinpoint the optimal path to attain the desired change in the current situation. Resolution is achieved by selecting a single course of action from a range of possible actions (Yasseri, 2012, p. 3).

4.2.5 Decision

According to Onwubiko (2016), the operator's responsibility lies in making decisions based on various inputs. These decisions are informed by accurately determining courses of action (CoA) and understanding the exact issues at hand. Tools and technology are utilized to synthesize, analyze, and process cues, information, and intelligence, leading to a conclusive set of responses. However, it's important to acknowledge that arriving at a conclusive response isn't always feasible due to incomplete, contradictory, or conflicting evidence, making decision-making challenging at times (Onwubiko, 2016, p. 8-9). Onwubiko (2016) states that decision-making involves considering multi-dimensional inputs to recommend a set of responses. Inputs include system factors, analysis outcomes from threat intelligence feeds, and alignment with the organization's vision, goals, and objectives. Additionally, reports provided by experts/operators are utilized to determine the most appropriate actions to address the situation (Onwubiko, 2016, p. 8-9).

4.2.6 System factors

System factors are technology-based functions, mechanisms, and techniques that help operators identify system-specific events. According to Onwubiko (2016) these may include environmental monitoring, scanning, sensor, and intrusion detection systems, which often automatically detect events in the environment and generate alerts. To form situational awareness, the information from these system factors often needs to be collected or integrated to understand the dependencies of events and to form a comprehensive picture (Onwubiko, 2016, p. 8).

4.2.7 Individual factors

The organization's level of investment in protecting its valued assets is driven by its vision, goals, and objectives. Onwubiko (2016) says that crucially, the risk appetite and tolerance of the organization are guided by the objectives, with goals serving as a metric for evaluating the return on investment. Attributes such as skills, experience, abilities, and training, collectively known as human factors, either enhance or influence operator situation awareness, whether on an individual or

group level, also referred to as team situation awareness. In order to generate suitable reports and identify courses of action to address issues, the operator or team must possess the skills and experience to analyze, assess, and process the cues they receive. This entails proficiency in utilizing specialized techniques, tools, and technology to manipulate and synthesize data and information, thereby enhancing intelligence gathering (Onwubiko, 2016, p. 8).

4.2.8 Adaption for cybersecurity

Based on the literature review, the Endsley's model is highly used as a base for different cybersecurity situational awareness studies. Endsley's model is adapted for the context of cybersecurity and visualized in different ways. One example where Endsley's model is adapted for the context of cybersecurity is a study of the Cyber-Attack Consequence Prediction. Datta, Lodinger et al. (2020) studied in their article about machine learning and natural language processing techniques to predict the consequences of cyberattacks. In their paper, Datta, Lodinger et al. (2020) describes Endley's model adaption in different way using circular process for cyber situational awareness. The model for cyber situational awareness, as depicted in Figure 7, illustrates its dimensions and process.

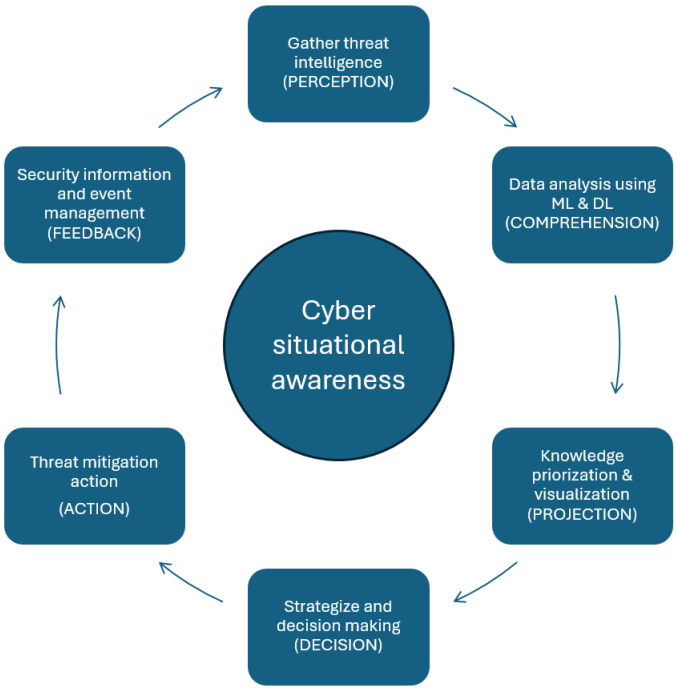

Figure 7 – Cybersecurity situational awareness model based on Endsley's SA model (adapted from Datta, Lodinger et al., 2020, p. 3)

It commences with gathering threat intelligence from diverse sources, including the current state of sensors in the CPS system and incident reports. According to Datta, Lodinger et al., (2020) following data collection, it's crucial for the security operation center to utilize automated tools equipped with cutting-edge machine and deep learning algorithms for data analysis, as highlighted in green in the figure, emphasizing the paper's main focus. Once the data is analyzed, the SOC can prioritize gathered knowledge and potentially visualize threat reports to devise strategies and make decisions in consultation with various stakeholders. Subsequently, after implementing appropriate actions, event logs and detailed action reports are archived in the security information and event management (SIEM) system for future reference and decision-making (Datta, Lodinger et al., 2020, p. 2-3).

4.3 Multi-level analysis framework for cybersecurity situational awareness

As the Endsley's model is one of the most adapted model for designing cybersecurity situational awareness, there are also some other models existed that are referred in some studies. Tianfield (2016) presented in his research after revisiting the concept of cyber security situational awareness (CSSA), an alignment of the process of CSSA with security data lifecycle and analyzed the requirements of CSSA (Tianfield, 2017, p. 2-3). He also presents a multi-level analysis framework for CSSA. The proposed requirements of Cybersecurity Situational Awareness in functional and system aspects are shown in Figure 8.

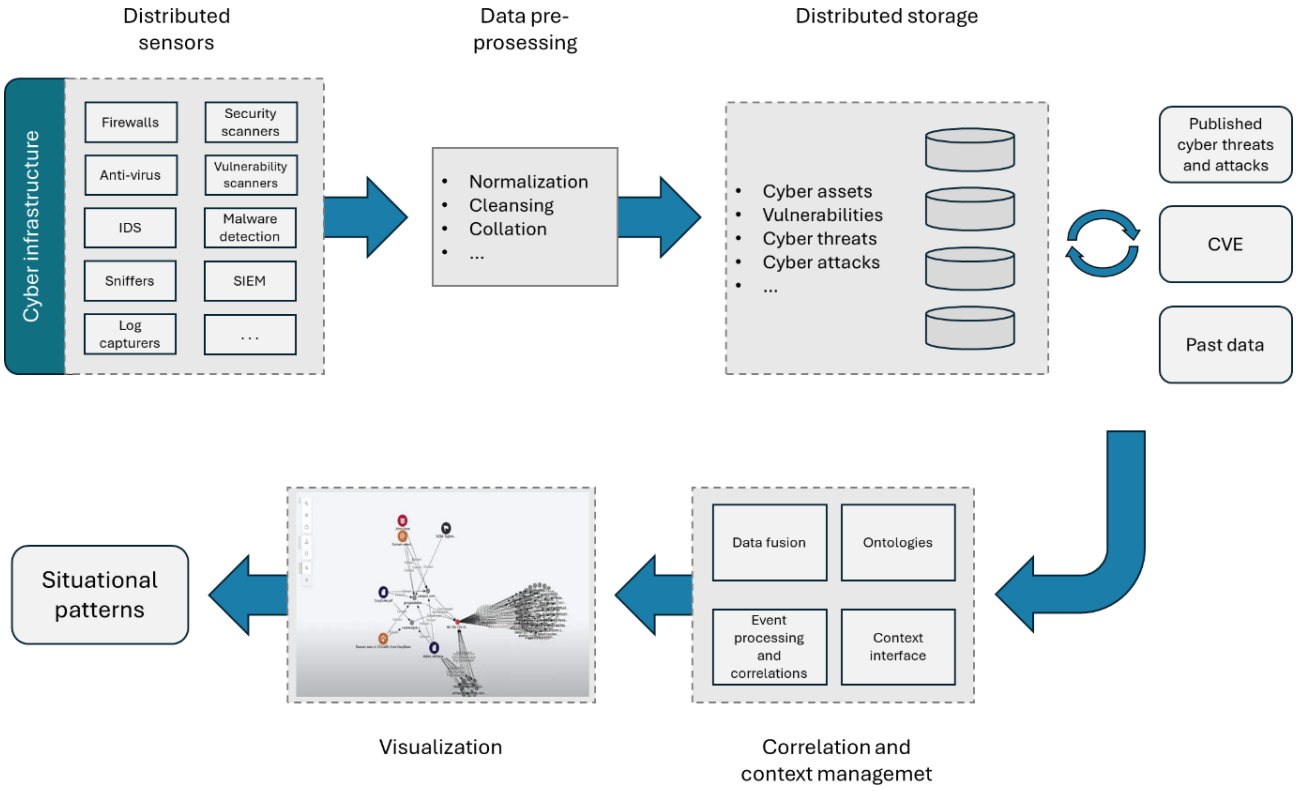

Figure 8 - Cybersecurity situational awareness requirements (adapted from Tianfield, 2016, p. 3)

The first step is to set up distributed sensors for the environment. Tianfield (2017) states that prior to implementing a distributed data storage system in an enterprise, it is crucial to deploy its components to facilitate the collection of both static and real-time event logs. Each organizational unit operates applications on its own clients, servers, and network devices such as intrusion detection/protection systems (IDS/IPS) and firewalls. The information gathered from these units is transmitted to a cyber security operations center (Tianfield, 2017, p. 2-3).

Once the data is collected, the next steps are pre-processing the data collected and storing it into distributed storages. Tianfield (2017) explains that all data is subjected to cleansing, normalization, and storage in a distributed structure, which can then be leveraged to support security information management and visualization. Data preprocessing includes tasks such as duplicate elimination, data calibration, and filtering of raw data from security sensors like IDS, firewalls, network and system logs, SIEM, and NetFlow records (Tianfield, 2017, p. 2-3).

The next step for CSSA is correlation and context management. In his study Tianfield (2017) states that during correlation and context processing, data fusion, event processing, and correlation occur. Data fusion aggregates evidence sets related to a perceived situation. The Dempster-Shafer evidence theory, a common fusion technique, synthesizes belief levels from individual data received from various sources to effectively reduce false positives and false negatives in security alerts. Moreover, data fusion techniques and complex event processing, which involve detecting and correlating events, can be employed to extract higher-level insights from the data (Tianfield, 2017, p. 2-3).

Tianfield (2017) concludes that security visualization entails transforming organized data and information into meaningful patterns or sequences for visualization. This process is a crucial component of the comprehension layer of situational awareness. By amalgamating all data and events to generate an integrated common picture, users can be engaged, immersed, and informed through a unified operational view supported by CSSA. This picture encompasses vulnerability, IT assets, risks, and real-time status information. Such a consolidated depiction of cybersecurity allows decision-makers to perform integrated risk analysis and effectively plan corrective actions (Tianfield, 2017, p. 2-3).

Tianfield (2017) presents in his article a proposed framework for cybersecurity situational awareness. Figure 9 illustrates the elevated tiers within the multi-level analysis framework of Cybersecurity Situational Awareness (CSSA). This framework includes data fusion, complex event processing, sequential pattern mining, pattern analysis, context inference, and management, among other components. These components extract higher-level insights from the data, facilitating situational assessment and projection (Tianfield, 2017, p. 4).

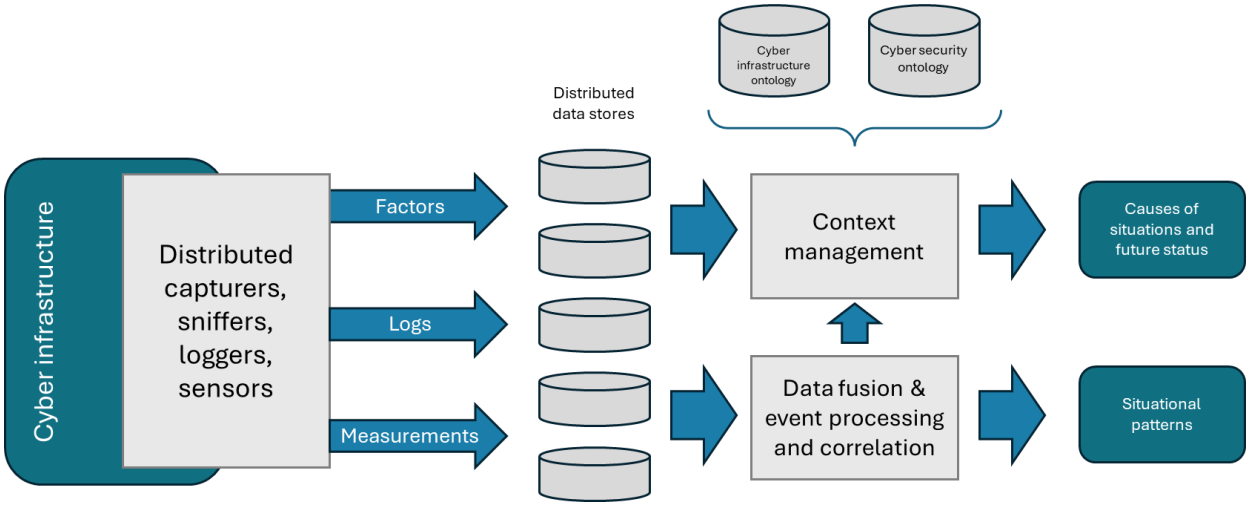

Figure 9 - Multi-level analysis framework of cybersecurity situational awareness (adapted from Tianfield, 2016, p. 4)

Data fusion and complex event processing correlate multiple factors to identify events related to the cyber infrastructure components and assets. Tianfield (2017 notes that by utilizing data from the distributed data store, data fusion constructs a comprehensive model of the cyber infrastructure, capturing its state and dependencies among components. In complex scenarios, data mining is employed to identify frequent patterns in security events. Situational assessment relies on analyzing sequential patterns in security events (Tianfield, 2017, p. 5).

Tianfield (2017) emphasizes that in the multi-level analysis framework of CSSA, it is crucial to differentiate between data fusion (e.g., based on Dempster-Shafer evidence theory) and event processing and correlation, versus data cleansing (e.g., duplicate elimination, data calibration, and filtering), normalization, and collation. The former focuses on extracting higher-level insights from the data, while the latter ensures the data's validity and accuracy (Tianfield, 2017, p. 5).

In the end, Tianfield (2017) states that projecting into the future is facilitated by leveraging the representation of the cyber infrastructure model in conjunction with semantic models. Context management, along with cyber infrastructure ontology and cybersecurity ontology, plays a crucial role by defining the semantic meaning of data and enabling inference capabilities related to cyber infrastructure components and assets (Tianfield, 2017, p. 5).

Additionally, inference capabilities extend to handling incomplete or conflicting information, enabling the propagation of component states to higher levels of dependent services. Tianfield (2017) says this results in the formation of a cyber infrastructure model that accurately reflects the state and dependencies over time. Visualizing the cyber infrastructure within a cyber operational picture provides stakeholders with rapid understanding, analysis, and decision-making capabilities (Tianfield, 2017, p. 5).

4.4 Cyber Common Operation Picture (CCOP)

Another model referred in other cybersecurity situational awareness studies, especially in military context is Common Operation Picture (COP). COP model has been extended to the context of cybersecurity in the concept of Cyber Common Operation Picture (CCOP or CyCOP).

According to Skopik, Bonitz et al. (2022) cyber common operating picture is essentially a curated set of information actively chosen to be beneficial for multiple stakeholders who share a common mission. Its purpose is to offer a unified perspective within the cyber domain, serving as a crucial element in establishing situational awareness regarding cybersecurity. Given the often complex and elusive nature of cyberspace, a CCOP plays a vital role in providing leaders with the necessary insights to make timely and informed decisions. Consequently, in the military context, the primary audience for CCOPs is typically at the command level, focusing on assessing the current status of the military organization's cyber assets (Skopik, Bonitz et al., 2022, p. 1321).

4.4.1 CCOP in strategical, operational and tactial level

CCOP can be created and presented in different levels based on the requirement and the target audience how will make the needed decisions. According to Skopik, Bonitz et al. (2022), CCOPs can serve different purposes and cater to various audiences. To comprehend their requirements fully, it's essential to understand the three target levels of a CCOP: operational, tactical, and strategic. This concept aligns with modern military theory, which divides warfare into these three levels. At the strategic level, the focus is on shaping and supporting national policy, while the operational level deals with the deployment of military forces within a theater of operations. The tactical level, on the other hand, involves the detailed execution of battles and responds to the dynamic aspects of ongoing engagements (Skopik, Bonitz et al., 2022, p. 1325).

Similar frameworks exist in other domains, such as decision-making. In the military context definition has been described in Skopik, Bonitz et al. (2022) paper as follows: "***Strategic*** *military decisions affect all or most of the organization and directly contribute to the achievement of the common goals of the organization*". Strategic management focuses on understanding the underlying causes of security problems and developing policies to address them. "***Tactical*** *military decisions serve the implementation of strategic decisions*". Tactical management deals with the implementation of security measures to mitigate these issues. "***Operational*** *military decisions are focused on day-to-day operations and a have a short-term horizon*". Operational management involves the practical application of security procedures and practices using specific tools and technologies. Skopik, Bonitz et al. (2022) states that these distinctions are also applicable in information security management. (Skopik, Bonitz et al., 2022, p. 1325).

4.4.2 CCOP requirements schema

To be able to utilize cyber common operation picture (CCOP) in decision-making it is crucial to understand the requirements for creating the CCOP. Skopik, Bonitz et al. (2022) suggest that CCOPs can vary significantly, and depending on their context of use, specific requirements emerge across five dimensions, particularly when they are employed to dynamically generate cyber security reports (Skopik, Bonitz et al., 2022, p. 1327).

Scope and Level: According to Skopik, Bonitz et al. (2022) situation report scope and target level shape CCOP development, influencing information source selection. Operational reports require more technical data, while strategic reports include broader external contextual data like political and economic information to prepare long-term decisions (Skopik, Bonitz et al., 2022, p. 1327).

Frequency and interval: Skopik, Bonitz et al. (2022) says that CCOPs should be regularly created (daily, weekly, monthly) and also available ad hoc during incidents, requiring a flexible process. However, ad hoc creation may lead to information loss, as snapshots capture only available data at one point, potentially resulting in incomplete or incorrect assessments, especially during ongoing attacks or cyber campaigns. (Skopik, Bonitz et al., 2022, p. 1327).

Output: In their study Skopik, Bonitz et al. (2022) states that the output of the CCOP process comprises various outcomes such as alerts, incident reports, or reports tailored to specific stakeholders. The recipient's needs greatly shape the content and level of detail in the situation assessment (Skopik, Bonitz et al., 2022, p. 1327).

Sources of information: In creating a CCOP, diverse information sources significantly impact situational assessment. Skopik, Bonitz et al. (2022) describes that these sources can be categorized as internal (pertaining to an organization's systems, services, and threat intelligence) and external (cyber threat data from purchased channels, partner organizations, and OSINT). While sources with suitable abstraction contribute directly to reports, technical data often require preparation before incorporation. For instance, threat intelligence may offer technical indicators, which, after analysis, are included in reports (Skopik, Bonitz et al., 2022, p. 1327).

Visualization: In the end, Skopik, Bonitz et al. (2022) writes that a CCOP should visualize the present status, past occurrences, sequential events, communication flow, and the national cyber scenario. This data can be presented through various means such as charts (bar, pie), trend graphs, color-coded systems, percentage tables, or geographical maps (Skopik, Bonitz et al., 2022, p. 1327). The visualization of situational awareness is addressed in this thesis more detail in chapter 4.5.

4.4.3 CCOP development process

Following the delineation of CCOP development requirements, Skopik, Bonitz et al. (2022) introduce a comprehensive model depicted in Figure 10. This model envisions diverse data and information streams entering the CCOP development process from multiple sources through various channels. Beyond data gathering, the intermediary phase involves data aggregation and interpretation, effectively converting data into actionable insights. Finally, the output phase represents these insights in a manner conducive to decision-making support (Skopik, Bonitz et al., 2022, p. 1327).

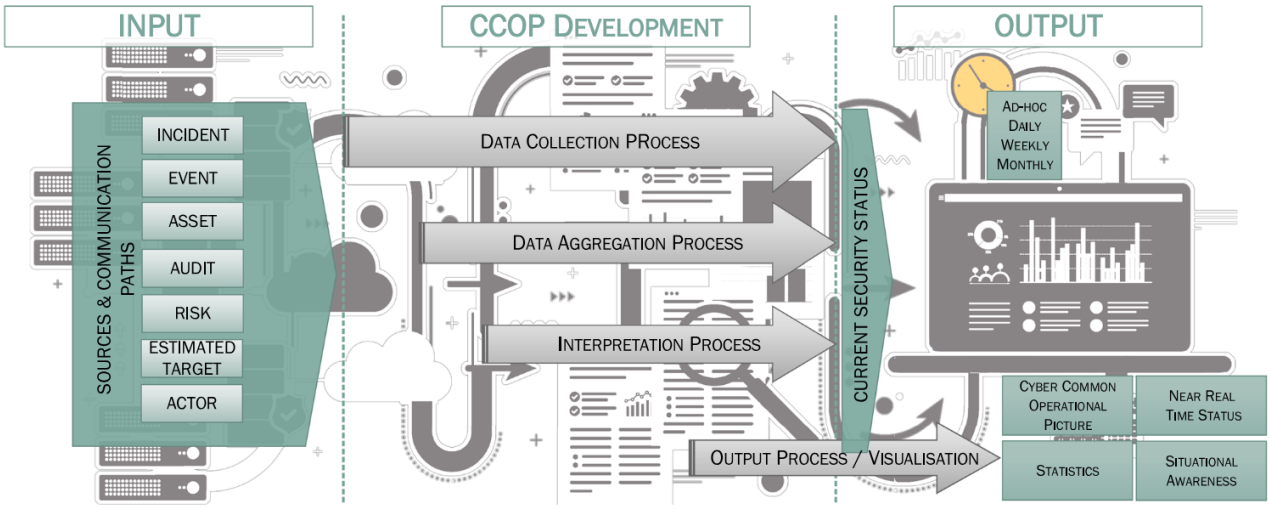

Figure 10 - Cyber Common Operation Picture (CCOP) development process (Skopik, Bonitz et al., 2022)

According to Skopik, Bonitz et al. (2022) in Cyber Situation Centers (CSCs), situation reports are crafted using diverse methods tailored to their specific purposes. For example, a report aiding in the assessment of a live incident differs from one forecasting the ramifications of a newly identified vulnerability. The main stages of the CCOP development process are as follows.

- Input: The input phase encompasses various sources and transmission pathways to integrate them into the CCOP development of the cyber situation center. Noteworthy sources contributing to CCOPs include incident tickets, asset information audit reports, identified risks, and threat actors with their anticipated objectives, based on recent research projects.
- CCOP Development Process: The general CCOP development process comprises four primary stages: data collection (inclusive of storing all pertinent information, messages, and historical reports), aggregation, interpretation, and output. The process of crafting a situation report initiates with data collection from diverse information sources, which occurs continuously given the unpredictable nature of cyber threats and attacks. The data collection process involves both automated and manual information retrieval. In the aggregation phase, data and information are categorized into predefined classes. The interpretation process entails identifying, analyzing, and evaluating the information relevant to the development process.

- Output: The final stage is the output phase, wherein reports are generated to meet the requirements of various stakeholders, timeframes, and formats. For instance, the current security status can be presented through reports, statistics, or dashboards on a daily, weekly, or monthly basis (Skopik, Bonitz et al., 2022, p. 1328).

In their research Skopik, Bonitz et al. (2022) introduce some example of data sources for the CCOP. These sources are divided into internal and external sources. Internal sources in their study Skopik, Bonitz et al. (2022) describes asset management information, CMDB information of monfiguration items, service catalog information of the cross-cutting services, workflow management system information, internal reports, incident handling information, internal audits including automated tests and penetration tests information and vulnerability management information. As an external data sources Skopik, Bonitz et al. (2022) describes external reports, open source intelligence (OSINT) information, cyber threat intelligence feeds and external audits (Skopik, Bonitz et al., 2022, p. 1328).

Application of CCOP process

In their research Skopik, Bonitz et al. (2022) outline a standard process for determining the overall security status, the Common Cyber Operating Picture (CCOP), which is commonly employed in Cyber Situation Centers (CSCs). Skopik, Bonitz et al. (2022) demonstrated their model in Austrian Ministry of Defense (MoD) organization context. Figure 11 illustrates the overarching process for generating the CCOP, based on the established approach used in the Austrian Ministry of Defense (MoD).

Skopik, Bonitz et al. (2022) states that the CCOP generation process involves two main perspectives relevant to the command level: an "external" view, which encompasses the global cyber situation with a focus on the national level, and an "internal" view, which examines all security-related processes, potential issues, and risks within the organization itself. Therefore, creating a CCOP entails two primary activities conducted simultaneously: (1) Assessing the general cyber situation, and (2) evaluating the security status of the organization through internal reports from specialized departments and other organizational units (Skopik, Bonitz et al., 2022, p. 1334-1335).

According to Skopik, Bonitz et al. (2022), to accomplish this, CSCs must leverage various information sources, including public sources such as news articles and OSINT feeds, as well as private or restricted sources like reports from partner organizations and internal departments. The process begins with gathering information from these sources and newly acquired sources undergo evaluation first (Skopik, Bonitz et al., 2022, p. 1334-1335).

Skopik, Bonitz et al. (2022) says that internal documentation from risk management and information security management, along with incident handling reports, vulnerability management statistics, and general service status information, are crucial components of the overall security status assessment and should be integrated into the CCOP (Skopik, Bonitz et al., 2022, p. 1334-1335).

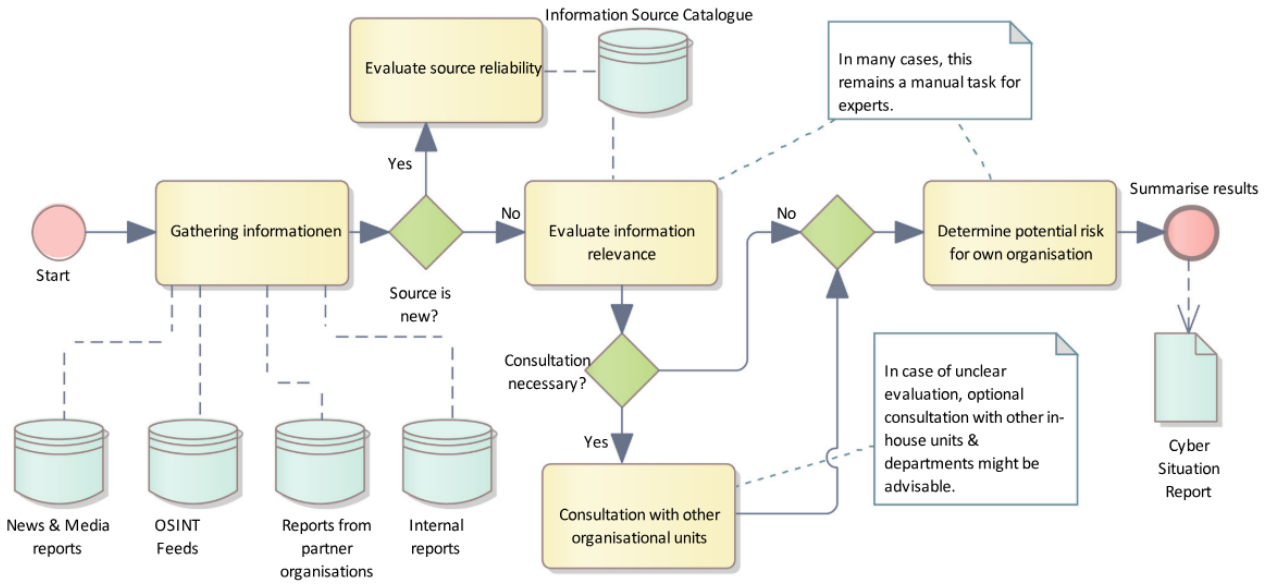

Figure 11 - Process for generating the CCOP (Skopik, Bonitz et al., 2022, p. 1335).

External information can be incorporated into your organization's information systems, Skopik, Bonitz et al. (2022) states. However, it's essential to evaluate this information to assess its risk accurately. As an example, Skopik, Bonitz et al. (2022) mentions, when new vulnerabilities emerge, it's crucial to determine if they could potentially impact your infrastructure. Similarly, if new threat actors emerge, it's necessary to ascertain if your organization fits their target profile. Additionally, when new Tactics, Techniques, and Procedures (TTPs) are identified, it's important to verify if they have been accounted for in your security controls. General events in the cybersecurity landscape

must also be examined to determine their relevance for informing the command level (Skopik, Bonitz et al., 2022, p. 1335).

The gathered information is then assessed for potential risks to your organization. According to Skopik, Bonitz et al. (2022) this evaluation can be performed manually or using machine learning techniques, and consultation with other organizational units may be necessary in some cases. The risk analysis should be tailored to the needs and characteristics of your organization, but it's recommended to follow established procedures such as ISO 27005 as an example. Considering factors like asset value, threat, and vulnerability can significantly enhance the informative value of the assessment. Additionally, a statistical evaluation of certain security-relevant metrics can be incorporated into the risk assessment. Finally, a report summarizing the results of the evaluation will be generated at the end of this process (Skopik, Bonitz et al., 2022, p. 1335).

4.5 Presenting and visualizing cybersecurity situational picture

In their presentation of the cyber situation awareness model, Datta, Lodinger et al. (2020) mentioned that based on data collection and analysis, threat reports are visualized during the projection phase for strategy planning and decision-making (Datta, Lodinger et al., 2020, p.2). Therefore, it is essential to be able to visualize and present the outputs generated by the situation awareness process in a way that is understandable, allowing conclusions to be drawn about the current state and potential future scenarios.

Kokkonen (2016) states in his study that one key challenge in cyber security situational awareness is how to effectively present the system's data to users, particularly for decision-makers who may lack deep technical expertise. Many cybersecurity tools are specialized and cater to specific data types, lacking interoperability with others. The key takeaway regarding visualization is the need for tailored tools and techniques suited to different purposes and user roles. Visualization tools for high-level decision-makers differ significantly from those for analysts (Kokkonen, 2016, p. 5)

One proposed solution to the visualization challenge involves the use of common symbols. Kokkonen (2016) suggests adopting military symbols, such as those outlined in standard MIL-STD-2525 and extending them for the cyber domain. For instance, a military symbol denoting pending identity could signify a new cyber incident. Establishing common symbols and adopting them as a

global standard for cybersecurity could enhance communication and understanding across the field (Kokkonen, 2016, p. 5).

Jiang, Jayatilaka et al. (2022) present a review of cyber situation awareness and visualization in their article. According the article, the complexity of cyber threats is on the rise, posing greater challenges for organizations seeking comprehensive insights into their cybersecurity posture. Consequently, organizations turn to Cyber Situational Awareness (CSA) to aid in comprehending cyber threats and their ramifications. Given the diverse and intricate nature of cybersecurity data, often characterized by multidimensional attributes, advanced visualization techniques are essential for achieving CSA (Jiang, Jayatilaka et al., 2022, p. 1).

Based on the research of Jiang, Jayatilaka et al. (2022) the majority of the reviews cited in their study either overlook Cyber Situational Awareness (CSA) entirely or focus solely on particular aspects of cyber security visualizations, such as network analysis or malware analysis. Consequently, the current literature reviews fail to offer a comprehensive perspective on CSA visualizations. Furthermore, they neglect to address crucial elements like the achievable level of Situational Awareness (SA) through visualization (i.e., mental states), the variety of stakeholders involved, the types of information depicted, and the challenges and best practices associated with CSA visualizations (Jiang, Jayatilaka et al., 2022, p. 1).

According to the article by Jiang, Jayatilaka, et al. (2022), the current state of visualizing cyber situational awareness primarily focuses on operational-level personnel, with a notable lack of visualizations aimed at other stakeholders such as higher-level decision-makers, managers and non-technical users. Most studies (92.6%) support the perception level, while several studies (53.7%) extend to the comprehension level. However, only a limited number of studies (18.5%) provide visualizations that reach the projection level, and just two studies offer CSA visualizations targeted at non-expert users. Their research also highlighted that external data sources are the least utilized in Cyber Situational Awareness (CSA) visualizations. This is concerning because relying solely on internal cybersecurity data and knowledge may restrict the comprehension of cyber security threats and risks, thereby impeding the effectiveness of cybersecurity decision-making (Jiang, Jayatilaka et al., 2022, p. 22).

Jiang, Jayatilaka et al. (2022) research review also builds upon Endsley's situation awareness model. While Endsley's model has been widely used and established for a long time, recent studies have highlighted other models for situational awareness visualization as well (Jiang, Jayatilaka et al., 2022, p. 3). One of these mentioned in the study is the Cyber-specific Common Operating Picture (CCOP or CyCOP). Throughout history, COP has been a military term denoting a command and control strategy that consolidates crucial operational data into a unified depiction, providing a common display of pertinent information shared among multiple commands. This approach fosters collaborative planning and aids decision-makers at all levels in attaining situational awareness (Jiang, Jayatilaka et al., 2022, p. 3).

Kookjin, Jaepil et al (2023) says in their article that CyCOP serves as a visualization instrument for the commander's cyber situational awareness, encompassing strategic, operational, and tactical/technical dimensions in its information presentation. It should integrate seamlessly with the current COP and possess a level of relevance adaptable to its users' preferences, including menus, symbols, and input methods. Moreover, it must effectively support the existing weapon system or Command and Control (C2) system utilizing cyberspace internally (Kookjin, Jaepil et al., 2023, p. 4). As an example from Kookjin, Jaepil et al (2023) study, in Figure 12 there is described how visualization is formed based on CyCOP model.

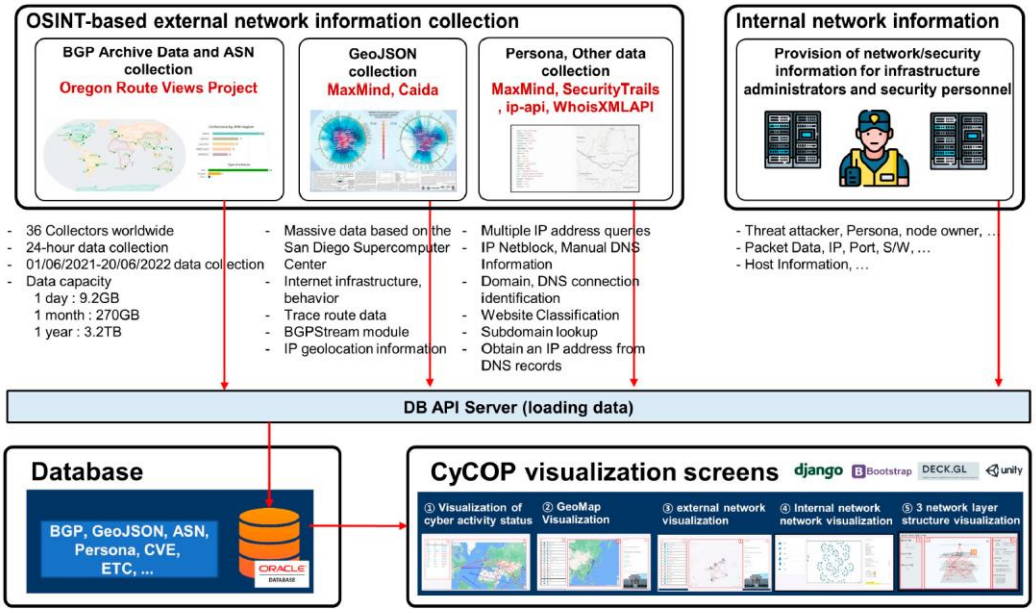

Figure 12 – Example of forming SA visualization based on CyCOP model (Kookjin, Jaepil et al., 2023, p. 11)

As a summary of current research about cyber security situational awareness visualization, it can be noted that there has been more focus on visualizing cyber situation awareness data from an operational perspective (perceive, comprehend) based on Endsley's model, while visualization of higher-level (projection) data has been less explored. It's important to visualize cyber situation awareness at different levels so that different stakeholders can make decisions on actions based on it. Although there are various technologies for visualizing cyber situation awareness, there is no identified general format or standard yet. In this study the interviews aim to explore the technologies currently used for visualizing cyber situation awareness.

4.6 Decision-making in cybersecurity

Datta, Lodinger et al. (2020) stated in their article that situation awareness is the concept of perceiving the elements in the environment, comprehending their meaning and making decisions or taking action (Datta, Lodinger et al., 2020, p. 1). Kokkonen, Hautamäki et al. (2016) says in their article that situation awareness plays a crucial role in decision-making within dynamic environments. While civil, commercial, and particularly military aviation have a long history of utilizing SA in decision-making processes, its importance extends to numerous other domains as well. Without accurate SA, even a skilled decision-maker is prone to making incorrect judgments (Kokkonen, Hautamäki et al., 2016, p. 2).

According to Kokkonen, Hautamäki et al. (2016) study, attaining comprehensive situation awareness within one's cyber domain is paramount, enabling the recognition of potential security threats, indicators of compromise (IOCs), and risk levels. Armed with this understanding, decision-makers can effectively steer their efforts towards cyber resilience, ensuring the uninterrupted operation and continuity of their business (Kokkonen, Hautamäki et al., 2016, p. 2).

Pöyhönen, Nuojua et al. (2019) states in their study of situational awareness and information sharing in critical infrastructure sector that organizations operate within intricate and interconnected cyber environments, utilizing both new and established information technology systems, such as systems of systems. These systems are essential for organizations to fulfill their missions, highlighting the critical dependency on them. Management must acknowledge that making clear, rational, and risk-based decisions is imperative for ensuring business continuity. Effective risk management involves integrating collective risk assessments from various individuals and groups

across the organization, spanning strategic planning to daily operational management. Understanding and managing risks are strategic capabilities and core responsibilities when organizing operations. This necessitates continuous awareness and comprehension of security risks at all levels of management. Security risks may not only target the organization's operations but also impact individuals, other organizations, and society as a whole. Therefore, proactive risk management is essential for safeguarding against potential threats and vulnerabilities (Pöyhönen, Nuojua et al., 2019, p. 239-240).

Based on the article of Pöyhönen, Nuojua et al. (2019) The Joint Task Force Transformation Initiative recommends a comprehensive approach to cyber risk management, addressing risks from strategic to tactical levels. This ensures that risk-based decision-making is integrated across all facets of the organization. The initiative emphasizes follow-up operations for risks at every decision-making level (Pöyhönen, Nuojua et al., 2019, p. 240).

At the tactical level, follow-up operations may involve ongoing threat evaluations to assess how changes in specific areas can impact strategic and operational levels. Pöyhönen, Nuojua et al. (2019) says that operational-level follow-up operations may entail analyzing new or existing technologies to identify risks to business continuity. Meanwhile, strategic-level follow-up operations often focus on information system entities, operational standardization, and continuous monitoring of security operations (Pöyhönen, Nuojua et al., 2019, p. 240).

As conclusion we can say that decision made in context of cybersecurity is in often based on situational awareness and threat intelligence information that are comprehended and visualized into understandable situational picture and reports. Decision should be based on risk assessment addressing the time, context, organization’s goals and critically of the situation regardless the organization level of the decision-making that are strategic, tactical and operational.

5 Cyber threat intelligence for situational awareness

Identifying cybersecurity threats plays a crucial role in forming the cyber situational awareness. According to the Security Committee's cybersecurity (2018) glossary, cybersecurity threats for an individual organization can include not only internal information system environments but also external factors, such as events and phenomena affecting society or critical infrastructure. In the cyber situational awareness process cycle model described by Datta, Lodninger et al. (2020), observation is based on intelligence gathering of cybersecurity threats (Datta, Lodinger et al., 2020, p. 2). Given the importance of intelligence gathering, detection of cybersecurity threats, and identification of their impacts in forming situational awareness, this section delves deeper into the topic of cybersecurity threat intelligence.

5.1 Cyber threat intelligence meaning

Based on the literature review there are many definitions and interpretations of what intelligence is or comprises. Ozkaya (2022) explains that according to the relevant US Army field manual, intelligence encompasses three main components:

- The product resulting from a series of activities, including collection, processing, integration, evaluation, analysis, and interpretation of available information pertaining to foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.
- The activities themselves that lead to the creation of this product.
- The organizations involved in carrying out these activities (Ozkaya, 2022, p. 2).

Based on Ozkaya (2022) threat intelligence refers to data that undergoes collection, processing, and analysis to comprehend a threat actor's motives, targets, and attack behaviors. Its purpose is to aid organizations in making data-driven security decisions and transitioning their cyber defense approach from reactive to proactive against threat actors. In today's highly digitalized world, where cyberattacks are commonplace, threat intelligence provides essential information for cybersecurity professionals to prevent and mitigate such attacks effectively. It equips professionals

with credible information necessary to fulfill their duties, enabling them to make informed decisions and take appropriate measures to address potential threats, ultimately averting potential business disasters (Ozkaya, 2022, p. 2).

Based on Abu, Selamat et al. (2018) Cyber Threat Intelligence (CTI) can be define "*comprehensively as evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat that can be used to inform decisions regarding the subject's response to that menace or hazard*" (Abu, Selamat et al., 2018, p. 373)

According to Borges Amaro, Percilio Azevedo et al. (2022) the concept of cyber threat intelligence (CTI) closely parallels the broader threat intelligence concept, involving the knowledge derived from various sources within the cybernetic field. CTI aims to assist security practitioners in identifying indicators of cyber-attacks, extracting information about attack methods, and subsequently responding to attacks accurately and promptly. Therefore, CTI professionals must possess skills in data extraction, filtration, manipulation, and standardization to achieve the crucial goal of generating and visualizing data intelligence in (preferably) real-time (Borges Amaro, Percilio Azevedo et al., 2022, p. 373).

Another key objective according to Borges Amaro, Percilio Azevedo et al. (2022) of CTI is to facilitate data sharing among stakeholders, as emphasized in. This promotes situational awareness among stakeholders by sharing information about the latest threats and vulnerabilities, enabling swift implementation of remedies to prevent others from experiencing the same threats or vulnerabilities that others have already encountered in the past. This objective helps to minimize redundant efforts, as threats already identified can be shared with all stakeholders, enhancing system defense against potential threats. Figure 13 outlines the steps and objectives that cyber threat intelligence should strive to achieve (Borges Amaro, Percilio Azevedo et al., 2022, p. 373).

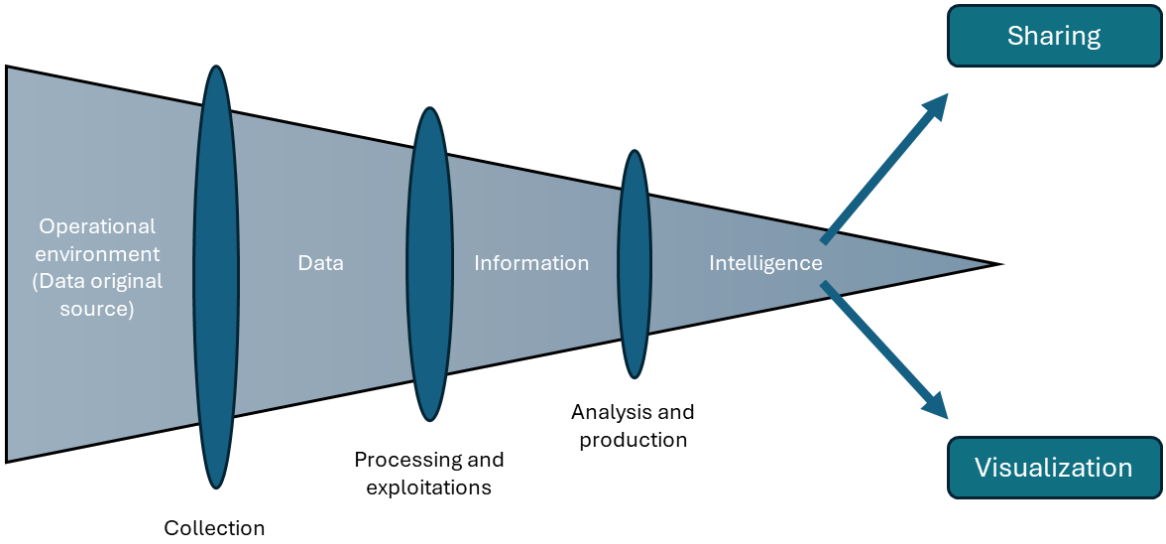

Figure 13 - Data traformation to intelligence (adapted from Borges Amaro, Percilio Azevedo et al., 2022, p. 374)

Ansile, Thompson, et al. (2023) argue that for the intelligence process to be effective, the final output must offer more value to decision-makers than the raw data. Intelligence is distinct from information in two crucial ways: it provides a level of prediction and guides decisions by emphasizing the variations in possible courses of action (Ansile, Thompson, et al., 2023, p. 3).

5.2 Threat intelligence types

Organizations can benefit from threat intelligence in four different ways. Both Ozkaya (2022) and Ansile, Thompson et al. (2023) describe four threat intelligence types that are strategic, tactical, operational, and technical (Ansile, Thompson et al., 2023, p. 4). Chrismon & Ruks (2015) also describes these four level in dimension of time and abstraction level. This aspect of the four CTI levels is presented in Figure 14.

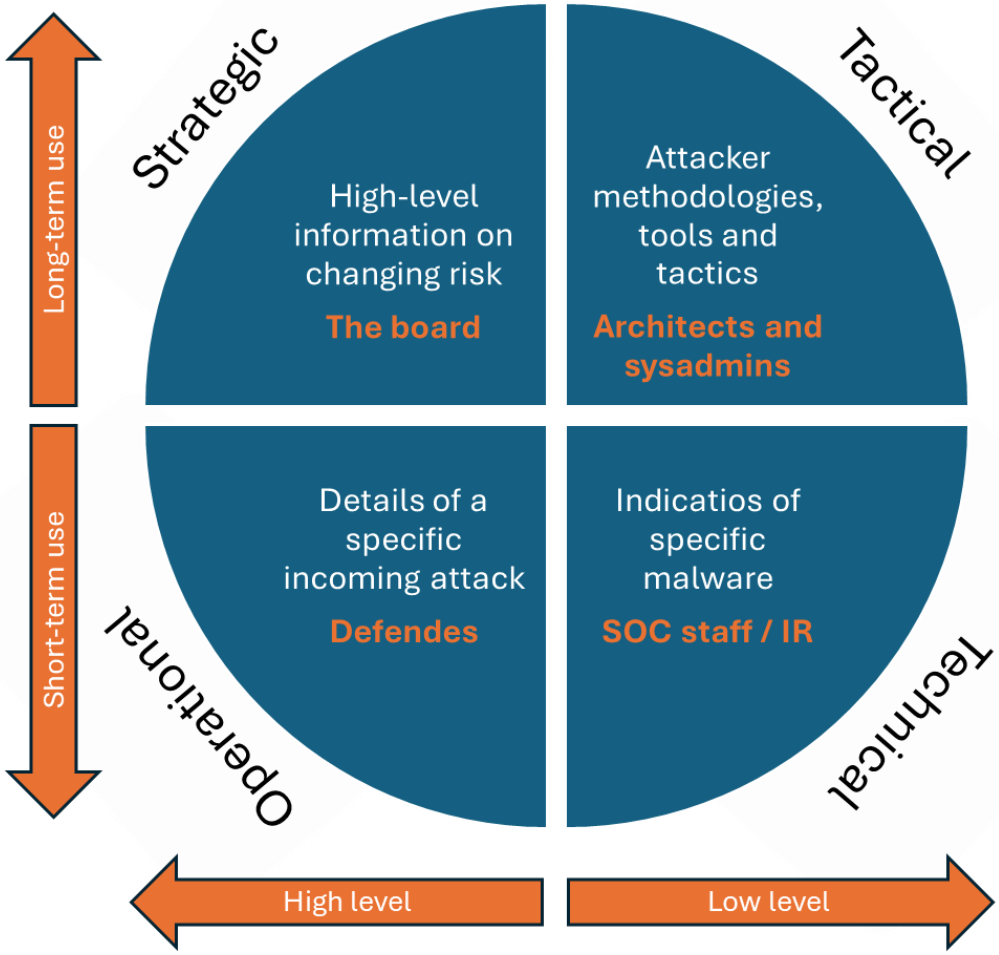

Figure 14 - Cyber threat intelligence types (adapted from Chrismon & Ruks, 2015, p. 6)

5.2.1 Strategic threat intelligence

According to Ozkaya's illustration (2022), in a strategic context, when one can determine high-level information about the risk of an attack, this insight is usually consumed by executives and managers due to its broader implications and strategic importance. This category of threat intelligence offers high-level insights that influence an organization's security posture, encompassing various threats, cyber-attack trends, financial risks, and business impacts. Typically consumed by high-level executives, it aids in managing an organization's IT functions, often overseen by the Chief Information Security Officer (CISO). Top management evaluates this strategic threat intelli-

gence concerning cyber risks, future uncertainties, involved threat actors, and overall business image impact. This intelligence furnishes top management with a report focusing on threats' risks and their long-term effects on business functions (Ozkaya, 2022, p. 4).

Strategic intelligence primarily emphasizes the enduring nature and consequences of threats on an organization's vital assets, such as IT infrastructure, customers, applications, and employees. Base on Ozkaya (2022) some types of information that fit in this category of threat intelligence include:

- The threat landscape for different industry sectors
- Geopolitical conflicts of different cyber attacks
- The financial effects of the cyber activities
- Threat actors and emerging cyber-attack trends
- Statistical data on breaches, malware, and data theft
- Information on changes in the threat landscape
- The effects on the business from various cyber-security decisions by top management (Ozkaya, 2022, p. 4)

5.2.2 Tactical threat intelligence

Ozkaya (2022) says that the category of tactical threat intelligence is dedicated to safeguarding an organization's assets and resources from potential attacks. It furnishes comprehensive details about attackers, including their techniques, procedures, and tactics employed in carrying out attacks. This level of intelligence is utilized by next-level managers within an organization, such as IT service managers, network operations employees, administrators, architects, and security operations managers. This intelligence provides the organization with insights into potential attacks, including attackers' capabilities, system vulnerabilities they might exploit, their objectives, and likely infiltration methods. Armed with this information, managers can devise defense systems and protective measures to mitigate cyber threats. Actions may include patching vulnerable systems and addressing identified weaknesses (Ozkaya, 2022, p. 5).

According to Ozkaya (2022) various sources provide tactical threat intelligence, including incident reports, campaign reports, malware analysis, human intelligence, and attack group reports. Intelligence is gathered through technical papers on cybersecurity issues, communication with different organizations (especially those within the same industry), or engagement with third-party cybersecurity specialists. This type of threat intelligence is often highly technical and intended for technical personnel capable of understanding information regarding malware, techniques, tools, campaigns, and various forensic reports (Ozkaya, 2022, p. 5).

5.2.3 Operational threat intelligence

Operational threat intelligence encompasses information highly specific to the organization, directly relating to its operations and past business actions. According to Ozkaya (2022) this intelligence aims to uncover the risks posed by various threats and attacks, providing insights into cyber attackers' methodologies for attempting system infiltration. It includes details of past security incidents affecting the company and any organizational changes made in response to those lapses. Additionally, it covers the economic aspects of addressing these security challenges. This type of intelligence serves organizations in several ways, including understanding potential threats, threat actors' capabilities, vulnerable assets, and attack opportunities. Government organizations typically express significant interest in this type of threat intelligence. The information aids security teams in planning security initiatives and deploying assets to address identified security vulnerabilities. The objective is to detect potential attacks early and take preventive measures to minimize harm to the organization's information assets (Ozkaya, 2022, p. 5).

Ozkaya (2022) says that operational threat intelligence is gathered from sources such as social media, chat rooms, human intelligence, and other real-world activities that may lead to cyber-attacks. It involves thorough evaluation of human behavior, cyber attackers, and related factors. Information obtained from such evaluations aids in predicting future attacks and supports the development of effective incident response plans. Operational intelligence typically contains details of malicious activities, recommended actions, and warnings of emerging attack trends (Ozkaya, 2022, p. 5).

5.2.4 Technical threat intelligence

Technical threat intelligence focuses on providing insights into the attacker's resources and methods of infiltrating systems. Ozkaya (2022) states that these details include command channels, tools, control channels, and more. Information obtained in this category typically has a limited lifespan compared to tactical or strategic intelligence and targets specific Indicators of Compromise (IoCs). The objective is to enable rapid response to threats (Ozkaya, 2022, p. 5).

As an example Ozkaya (2022) says, if an attacker uses malware to infiltrate a system, the malware itself constitutes tactical threat intelligence. However, the specific methods the attacker intends to employ with the malware to infiltrate systems qualify as technical intelligence. This may include specific IP addresses and techniques such as phishing email headers used in attacks (Ozkaya, 2022, p. 5).

Based on Ozkaya (2022) article, sources for gathering this type of intelligence include data feeds from external third parties, active campaigns, and shared attack information from other organizations. This information aids security teams in adding additional IoCs to their systems to identify security breaches and enhance the organization's security posture. It also assists in identifying malicious IP addresses for blacklisting or detecting attackers based on geographical irregularities. Intelligence gathered is directly input into security devices to aid in blocking suspicious inbound or outbound traffic (Ozkaya, 2022, p. 5).

5.3 Cyber threat intelligence life cycle

Executing cyber threat intelligence is often based on process or a model of CTI life cycle. Ozkaya (2022) introduces in his article a process for generating threat intelligence. The process of generating threat intelligence involves a cycle aimed at transforming raw collected data into actionable intelligence that enhances the organization's security posture. This development of intelligence is a knowledge-intensive process involving the identification of new questions and gaps, followed by the determination of new requirements. Subsequently, an iterative process ensues, leading to the generation of valuable intelligence. The iterative nature of CTI process is crucial as it ensures that the generated knowledge becomes increasingly refined over time. Challenges are identified and addressed with each iteration, allowing for continuous improvement. Each iteration builds upon

the previous one, resulting in more sophisticated and insightful intelligence (Ozkaya, 2022, p. 6). The process includes six steps that are shown in Figure 15.

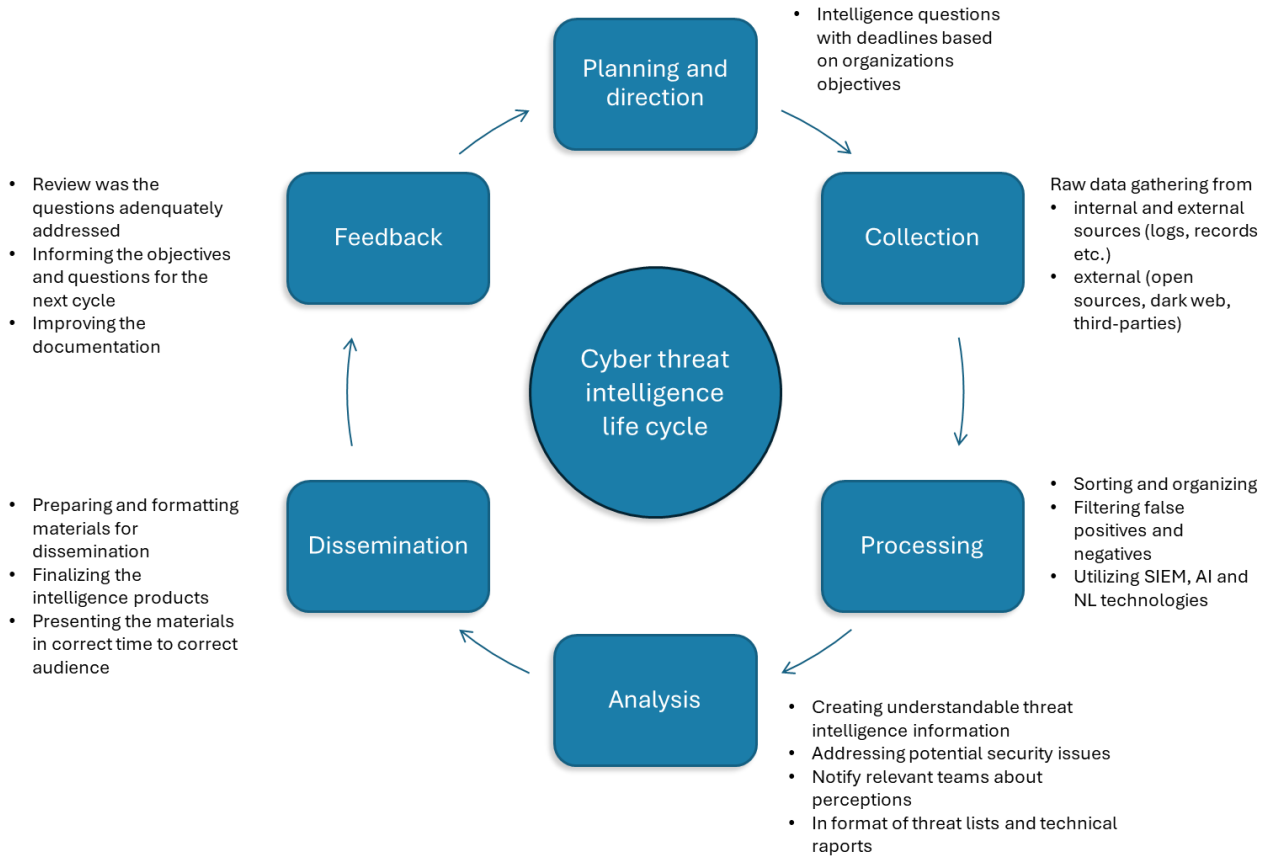

Figure 15 - Threat intelligence life cycle (adapted from Ozkaya, 2022, p. 6)

Comparing Cyber threat intelligence life cycle to Endsley's model of situational awareness, there can be seen lots of similarities. In both processes the end results of the processes are based on data collection from the cyber environment, making the analysis of the information collected and processed. Both processes give feedback to the data collection planning. This states that cyber threat intelligence supports well the cyber situation model of Endley's. The cyber threat intelligence process doesn't describe decision making as its own stage nor it is seen included for the dissemination stage.

5.3.1 Planning and direction

The initial phase in generating valuable intelligence involves formulating precise questions. Based on Ozkaya (2022) these questions should be focused on singular issues, events, facts, or activities, avoiding open-ended queries that may yield a broad spectrum of answers. Structuring questions based on the organization's objectives is crucial, as the answers should align with these objectives. Additionally, Ozkaya (2022) states that consideration should be given to deadlines for obtaining answers and the impact these answers will have on the organization's objectives. This assessment aids in prioritizing intelligence generation objectives. The primary consideration at this stage is identifying the beneficiaries of intelligence, typically either top management seeking broad threat insights or technical experts seeking specific exploit information. The nature and depth of the intelligence generation process will vary based on these categories (Ozkaya, 2022, p. 7).

Based on Ainslie, Thompson et al. (2023) 'Direction' in intelligence process denotes the purpose behind the intelligence needed to facilitate the activity. Each stakeholder offers input on the specific questions they require answers to, and these parameters define the information requirements, including their priority. Determining the most suitable sources and methods for obtaining the information forms the basis of planning for information collection, which is the subsequent stage of the cycle (Ainslie, Thompson et al., 2023, p. 7).

5.3.2 Data collection

Following the delineation of requirements in the planning phase, the next step involves gathering raw data to fulfill these requirements. Ainslie, Thompson et al. (2023) says that during the collection phase, efforts are focused on gathering all the information needed to fulfill the requirements from various sources and agencies that are most appropriate for the task (Ainslie, Thompson et al., 2023, p. 3). According to Ozkaya (2022), a diverse range of sources, both internal and external, should be utilized for this purpose. Internal sources provide network event logs and records of past incident responses, while external sources include the open and dark web, as well as third-party cyber-security consultants. Data collected may include malicious IP addresses, domains, indicators of compromise (IoCs), file hashes, vulnerability information, personally identifiable information, code from paste sites, and data from social media and news sources (Ozkaya, 2022, p. 7).

5.3.3 Processing

The Processing phase is a critical and complex activity whereby information is synthesized into intelligence (Ainslie, Thompson et al., 2023, p. 3). Ozkaya (2022) states that once the data is collected, it undergoes sorting, organization with metadata tags, and filtering to eliminate redundant information, false positives, and negatives. With the vast volume of data generated daily, automated tools such as Security Information and Event Management (SIEM) systems are essential for efficient analysis. While SIEM tools are effective, they may be inadequate when dealing with diverse data sources. Hence, more robust solutions, such as machine learning and natural language processing tools, are recommended for processing and structuring unstructured data from various sources (Ozkaya, 2022, p. 7).

5.3.4 Analysis and production

Following processing, the next step involves making sense of the data to identify potential security issues. According to Ozkaya (2022) the objective is to notify relevant teams of this information in formats aligning with the outlined intelligence requirements. The format of threat intelligence information may vary based on objectives and audience preferences, ranging from simple threat lists to complex, technical reports tailored for technical audiences. The key is to present the data in a format understandable to the intended audience (Ozkaya, 2022, p. 7).

5.3.5 Intelligence dissemination

During this phase, Ainslie, Thompson et al. (2023) states that pertinent, timely, and prognostic material is meticulously prepared and formatted to ensure accuracy and usability before being disseminated to those who require it to make decisions based on the intelligence gleaned from the preceding processes (Ainslie, Thompson et al., 2023, p. 3). Ozkaya (2022) says that following the analysis of data, the finalized product, namely threat intelligence, is presented to its intended audience. Timing is crucial for threat intelligence to be actionable and beneficial, necessitating its delivery to the target audience promptly. Tracking becomes imperative at this stage to ensure continuity across different intelligence cycles. This ensures that past challenges are acknowledged, and any lessons learned are retained and integrated into subsequent cycles. Ticket systems play a vital role in this process, facilitating the integration of the intelligence cycle with other security systems within the organization. This integration ensures that whenever an intelligence ticket is generated,

it undergoes proper submission, documentation, review, and fulfillment by multiple stakeholders across the organization. These stakeholders work collaboratively towards a common objective: enhancing the organization's security posture (Ozkaya, 2022, p. 8).

5.3.6 Feedback

The final step of the cycle serves to complete the full circle of the life cycle by linking it back to the initial planning and direction phases. According to Ozkaya (2022) ideally, the product is presented to the original requester for review, allowing them to assess whether their questions have been adequately addressed. This connection between the final product and the initial steps confirms whether the objectives have been achieved, while also informing the objectives and questions for the next cycle. Additionally, it contributes to improving documentation and ensuring the continuity of processes, which is crucial for the learning curve that ultimately enhances current processes (Ozkaya, 2022, p. 8).

6 Co-operation and information sharing of cybersecurity situational awareness

Co-operation and information sharing with stakeholders can be seen an important function of good quality situational awareness. As Borges Amaro, Percilio Azevedo et al. (2022) mentioned before facilitating data sharing among stakeholders is one of the key objective of cyber threat intelligence which promotes situational awareness among stakeholders by sharing information about the latest threats and vulnerabilities, enabling swift implementation of remedies to prevent others from experiencing the same threats or vulnerabilities that others have already encountered in the past (Borges Amaro, Percilio Azevedo et al , 2022). As information sharing is seen a key element for building comprehensive situational picture, this chapter reviews in detail the benefits and challenges of information sharing in context of cybersecurity. We also introduce standardization of threat information sharing.

6.1 Advantages and challenges of cybersecurity information sharing

Kokkonen (2016) says in his article that in cybersecurity, information sharing stands out as a cornerstone. When operating within a network of trusted organizations, the potential for data fusion significantly expands. However, this necessitates filtering shared information in line with company policies. Due to the sensitivity of security data, not all information can be disclosed. Moreover, incoming data must undergo analysis, with reliability scores assigned accordingly. Standards like Structured Threat Information eXpression (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™) have been established for the exchange of cyber threat information (Kokkonen, 2016, p. 5).

Rizov (2018) in his publication, explores the advantages and obstacles associated with coordinating and exchanging cyber threat information. He delves into the merits and limitations of various information sharing models, highlighting their respective strengths and weaknesses. According to Rizov (2018) the five Rizov's stated benefits of exchanging cyber threat information are

1. **Shared Situational Awareness**: Collaborative information sharing enables organizations to tap into the collective knowledge, experiences, and analytical capabilities of their sharing

partners. This collective awareness strengthens the defense capabilities of multiple organizations within a community, with even a single contribution enhancing the security posture of the entire group.

2. **Enhanced Threat Understanding:** By exchanging and developing threat information, organizations gain deeper insights into the threat landscape. Shared information informs cybersecurity and risk management practices, aiding in the identification of affected systems, implementation of protective measures, improvement of detection capabilities, and more effective incident response and recovery strategies.
3. **Knowledge Maturation:** Sharing seemingly unrelated observations allows organizations to correlate data collected by various entities. This enrichment process increases the value of information by refining existing indicators and developing a better understanding of threat actor Tactics, Techniques, and Procedures (TTPs) associated with specific incidents or campaigns. Correlation also provides insights into the relationships between various indicators.
4. **Herd Immunity:** Analogous to the concept of community immunity in biology, organizations that act upon received threat information by remedying threats to themselves contribute to a collective defense. This proactive approach reduces the number of viable attack vectors for threat actors, thereby enhancing overall resilience and protecting entities that may not have received or acted upon the shared threat information.
5. **Greater Defensive Agility:** Threat actors continuously adapt their TTPs to evade detection and exploit vulnerabilities. Organizations engaged in information sharing are better positioned to stay informed about evolving TTPs and can swiftly detect and respond to emerging threats. This agility not only strengthens defenses but also increases the cost for threat actors by necessitating the development of new tactics and techniques (Rizov, 2018, p. 45-46).

Rizov (2018) presents in his articles the major types of cyber threat information that are Indicators, security alerts, tactics, techniques, and procedures, tool configurations and threat intelligence reports (Rizov, 2018, p. 46). As in the disadvantages or challenges Rizov (2018) claims in his article as follows:

1. **Establishing Trust:** Building trusted relationships is paramount for successful information sharing but requires continuous effort to establish and maintain. Regular communication, whether through in-person meetings, phone calls, or social media, accelerates the trust-building process.
2. **Achieving Interoperability**: Standardized data formats and transport protocols are crucial for interoperability, facilitating secure and automated exchange of structured threat information among organizations, repositories, and tools. However, adopting specific formats and protocols may demand significant time and resources, and the value of these investments may diminish if sharing partners require different standards.
3. **Protecting Sensitive Information:** Disclosure of sensitive information, such as intellectual property or trade secrets, can lead to financial loss, reputational damage, and violation of agreements. Unauthorized disclosure may disrupt ongoing investigations or response actions. Organizations should designate handling procedures for shared information and implement policies, procedures, and technical controls to actively manage risks associated with sensitive but unclassified data.
4. **Protecting Classified Information:** Accessing classified data can be complex and costly. Organizations must navigate clearance requirements and restrictions, especially for individuals without appropriate clearances or from countries lacking mutual protection agreements (Rizov, 2018, p. 47-48).

As stated by Rizov (2018), for organizations it is important to understand what information they can share with their stakeholders and what information is classified and be shared with more caution (Rizov, 2018, p. 47-48). Kokkonen, Hautamäki et al. (2016) says in their study that it's commonly believed that organizations exchange classified security data. However, there's a constant concern that such information sharing might lead to misuse. Establishing trust between diverse organizations is the primary challenge in real-world information sharing, especially when it involves sensitive and classified security data (Kokkonen, Hautamäki et al., 2016, p. 3-4). Kokkonen, Hautamäki et al. (2016) has introduced their model for information sharing risk calculation that can be used for defining paths for information sharing and choosing the lowest risk level topologies. This model has been demonstrated in healthcare domain by Hautamäki & Kokkonen (2019). Hautamäki & Kokkonen (2019) says that healthcare sector is highly digitalized domain as a part of mission critical infrastructure where cyber-attacks can cause extreme circumstances. Decision-

making necessitates an understanding of the current situation. This is especially true in the intricate field of cybersecurity, where traditional physical boundaries are absent, making situational awareness crucial. One essential source of the necessary cybersecurity information comes from information sharing. The demonstration highlighted the model's applicability within a single country or across borders, particularly when "higher authorities" with international connections are engaged. Effective information sharing necessitates clear classification levels for the shared data (Hautamäki & Kokkonen, 2019, p. 2-5).

6.2 Information sharing in cybersecurity situational awareness systems

Kokkonen (2016) has studied in his article about cyber security situational awareness systems what information sharing is one of the key functions. He introduces a proposed architecture for cyber security situational awareness systems. This architecture is presented in Figure 16. The proposed architecture signifies a cutting-edge system in the cyber security domain, integrating both data fusion engines and data exchange mechanisms concurrently. For fusion of multi sensor data, the proposed architecture uses Joint Directors of Laboratories (JDL) model where the fusion process is divided into six different levels (Kokkonen, 2016, p. 3-8).

The architecture offers the flexibility to implement all levels of the JDL data fusion process, including the highest tiers, as part of the Situational Awareness framework. Additionally, the visualization component can be structured into layers to cater to the diverse requirements of various user roles, such as decision-makers and analysts, ensuring optimal support for their distinct needs (Kokkonen, 2016, p. 3-8).

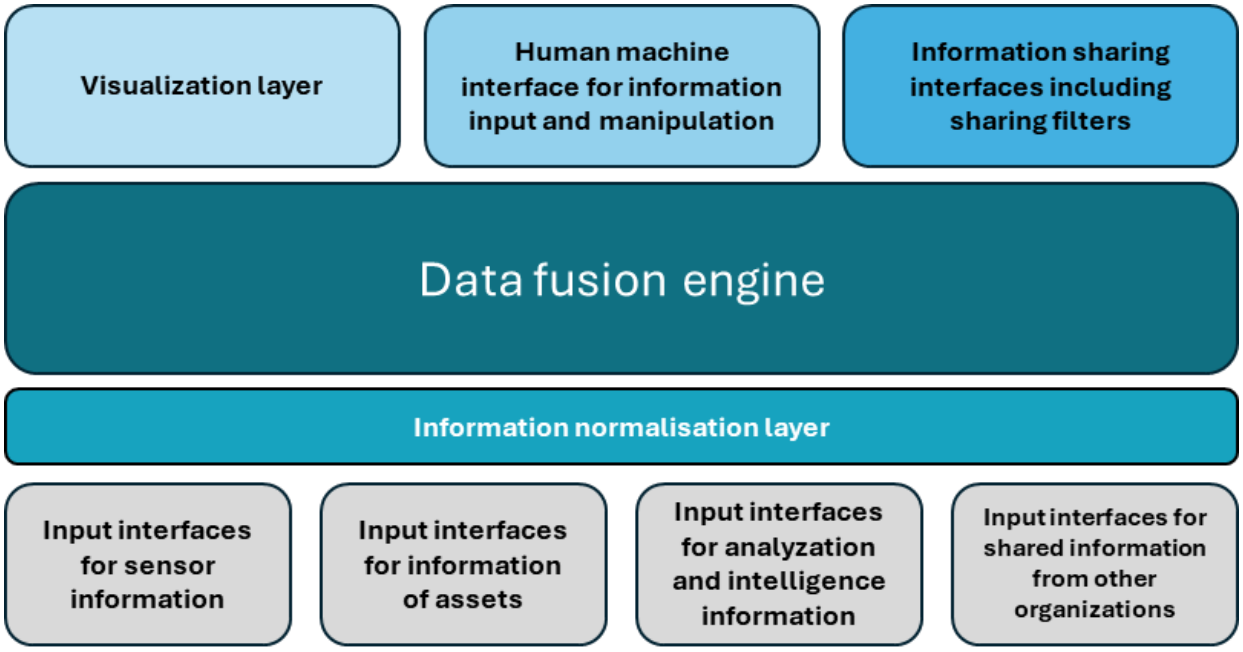

Figure 16 - Cybersecurity situational awareness system architecture (adapted from Kokkonen, 2016, p. 6)

Kokkonen (2016) claims that in cyber security, information sharing is pivotal, facilitating a collective defense against threats. When a trusted network of organizations exists with the capacity to share information, data fusion capabilities are greatly enhanced. However, shared information must undergo filtering according to company policies to safeguard sensitive data. Not all information can be shared due to confidentiality concerns. Additionally, inbound data should be analyzed, and reliability scores assigned to ensure the quality and trustworthiness of the shared information (Kokkonen, 2016, p. 5). Based on Kokkonen (2016) information shared by other organizations is described in the architect as one of the four main input interfaces of the CSA systems. Also, the architecture presents information sharing as output interfaces to share situational awareness information to the information sharing community. Kokkonen (2016) says that while the ultimate aim of such systems is to automate functionalities as much as possible, the presence of analyst operators remains necessary. These operators are responsible for overseeing data fusion, managing sensors, and integrating analysis information into the system (Kokkonen, 2016, p. 8).

6.3 Mitre TAXII model and STIX language for threat information sharing

Based on MITRE (2015) the challenge of cyber threat intelligence lies in the fact that no single organization possesses enough relevant information to fully comprehend the threat landscape. To address this, sharing relevant cyber threat information among trusted partners and communities is essential. Through such sharing, each partner gains a more comprehensive understanding of the threat landscape, enabling them to identify specific indicators of attack (The MITRE Corporation, 2012, p. 2).

According to MITRE (2012) given the dynamic nature of the threat landscape and the rapid pace of events, automation is crucial for effective analysis and response. Automation requires high-quality data feeds, and defensive capabilities often rely on a diverse range of products and systems. Standardized, structured representations of threat information are necessary to facilitate information sharing among a broad community of sources (The MITRE Corporation, 2012, p. 2).

MITRE (2012) highlights that one of the key challenges faced by threat-sharing organizations is achieving standardization without sacrificing human judgment and control. To address this, there is a need for standardized representations of structured threat information that are expressive, flexible, extensible, automatable, and readable. MITRE has developed a community-driven solution to this challenge with the Structured Threat Information eXpression (STIX) framework (The MITRE Corporation, 2012, p. 2). The Trusted Automated eXchange of Indicator Information (TAXII™) serves as the primary means for exchanging information encoded in the STIX Language. It empowers organizations to securely and automatically share structured cyber threat information (The MITRE Corporation, 2013).

Pahlevan, Voulkidis et al. (2021) says that TAXII was introduced as a suite of protocols and technical documents designed to facilitate the exchange of relevant Cyber Threat Intelligence (CTI) among organizations and different sectors of industry. It achieves this by specifying data formats and secure transport mechanisms for sharing threat information, which is subsequently utilized for real-time detection, prevention, and mitigation of cyberattacks (Pahlevan, Voulkidis et al., 2021, p. 4).

According to Pahlevan, Voulkidis et al. (2021) from a technological standpoint, TAXII functions as an application protocol and service specification for CTI exchange over HTTPS. As such, it adheres to a client-server model and outlines requirements for both service clients and servers. Implemented as a RESTful API, TAXII offers a range of services and message exchanges. Two primary services defined by TAXII cover various cyber threat information sharing scenarios:

1. **Collection**: This service acts as an interface to a logical repository of CTI objects maintained by a TAXII server on behalf of CTI producers. It follows a request-response model for communication between TAXII clients and servers.
2. **Channel**: Similar to a collection, a channel is maintained by a TAXII server and allows CTI producers to publish threat information to multiple consumers simultaneously. It enables consumers to receive CTI from various producers and adopts a publish-subscribe communication model for threat information exchange. However, it's worth noting that the latest version of the TAXII standard (v2.1) does not support Channel services yet (Pahlevan, Voulkidis et al., 2021, p. 3).

In their research, Pahlevan, Voulkidis, et al. (2021) explain that TAXII, originally designed to facilitate the exchange of cyber threat intelligence formatted as STIX objects, requires support for transporting STIX objects. However, TAXII can also be used to exchange threat information in other formats through TAXII messages. STIX and TAXII are independent standards, meaning that the formats and serializations of STIX objects were not specifically defined with any particular transport protocols in mind, and TAXII can facilitate the sharing of non-STIX data as well (Pahlevan, Voulkidis, et al., 2021, p. 4).

The authors believe that widespread adoption of TAXII could result in significant operational improvements, smooth compatibility with existing sharing policies, and the ability to cover various threat sharing paradigms, such as peer-to-peer and source-subscriber models (Pahlevan, Voulkidis, et al., 2021, p. 4). They propose an approach to enhance the secure and real-time exchange of cyber threat information by extending the technological capabilities of the TAXII framework and addressing its limitations through the integration of Distributed Ledger Technologies (DLT) and a generalized publish-subscribe middleware (Pahlevan, Voulkidis, et al., 2021, p. 4).

The solution of Pahlevan, Voulkidis et al. (2021) aims to provide a more robust and efficient mechanism for sharing cyber threat information, leveraging the inherent security and transparency features of DLTs. By integrating DLTs into the TAXII framework, they enhance the trustworthiness and immutability of the exchanged threat data while also ensuring real-time dissemination. The proposed solution has undergone validation in several use cases tailored to the specific requirements of Electrical Power and Energy Systems. These use cases demonstrate the practical applicability and effectiveness of the proposed approach in addressing the unique challenges faced by critical infrastructure sectors (Pahlevan, Voulkidis et al., 2021, p. 1).

According to The Mitre Corporation (2012) the Structured Threat Information eXpression framework (STIX), developed collaboratively with all interested parties, serves as a language for specifying, capturing, characterizing, and communicating standardized cyber threat information. Its structured approach enhances cyber threat management processes and facilitates automation. By offering a standardized mechanism for handling structured cyber threat information across various use cases, STIX enhances consistency, efficiency, interoperability, and overall situational awareness. Furthermore, STIX offers a unified architecture that connects diverse cyber threat information sources (The MITRE Corporation, 2012, p. 5-7). Based on Mitre, STIX is targeted to support a range of core use cases involved in cyber threat management, that are presented in Figure 17.

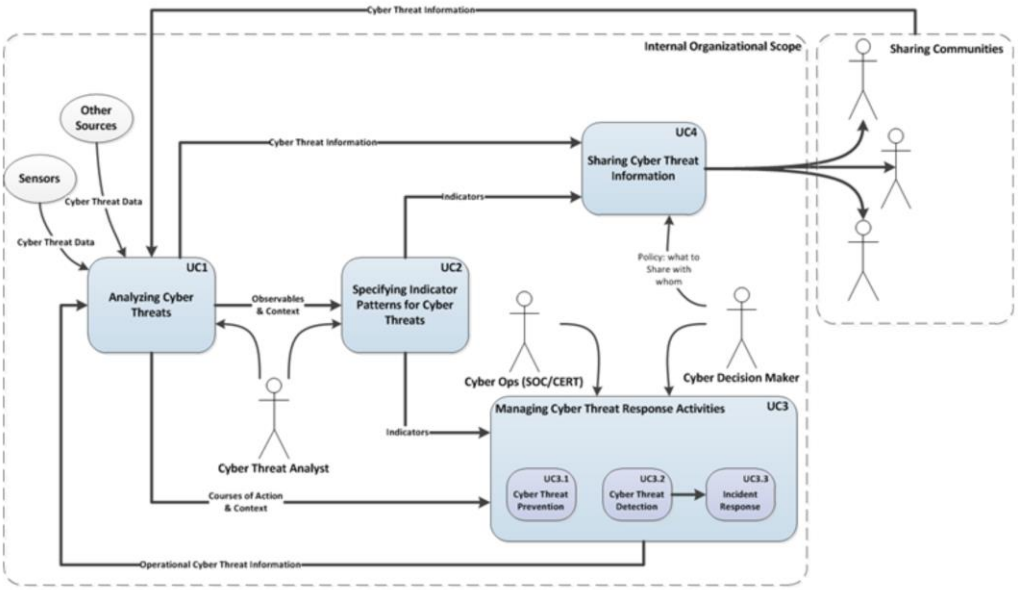

Figure 17 - STIX use cases (The MITRE Corporation, 2012, p. 6)

Analyzing Cyber Threats, use case 1 - A cyber threat analyst meticulously examines both structured and unstructured data pertaining to cyber threat activity, sourced from manual or automated channels. According to The MITRE Corporation (2012) the objective is to grasp the essence of pertinent threats, pinpoint them, and thoroughly characterize them to ensure all relevant aspects of the threat are fully articulated and can evolve over time. This encompasses understanding threat-related actions, behaviors, capabilities, intentions, attributed actors, and more. With this comprehensive understanding and characterization, the analyst can propose relevant threat indicator patterns, recommend courses of action for responding to threats, and/or share this information with other trusted parties (The MITRE Corporation, 2012, p. 6).

Specifying Indicator Patterns for Cyber Threats, use case 2 – Based on The MITRE Corporation (2012) a cyber threat analyst defines quantifiable patterns that encapsulate the observable attributes of particular cyber threats, alongside their contextual information and pertinent metadata for interpreting, managing, and utilizing the pattern and its matched outcomes. This process can be carried out either manually or with the aid of automated tools, and it involves structuring substantial threat information (The MITRE Corporation, 2012, p. 7).

Managing Cyber Threat Response Activities, use case 3 - Cyber decision-makers and cyber operations personnel collaborate to thwart or identify cyber threat activity, as well as to probe and address any detected instances of such activity. According to The MITRE Corporation (2012) preventive actions may involve remedial measures aimed at mitigating vulnerabilities, weaknesses, or misconfigurations that could be exploited. Subsequently, following the detection and investigation of particular incidents, reactive measures may be pursued. In cyber threat prevention (use case 3.1) cyber decision-makers assess potential preventive measures for identified threats and choose suitable actions for deployment. Cyber operations personnel then execute these selected measures to thwart specific cyber threats. This could involve implementing general mitigations as a proactive measure or deploying targeted countermeasures based on predictive analysis of leading indicators. In cyber threat detection (use case 3.2) cyber operations personnel employ various mechanisms, including both automated tools and manual processes, to monitor and evaluate cyber operations. Their goal is to identify specific cyber threats, whether they occurred in the past based on historical data, are currently unfolding through real-time situational awareness, or are anticipated through predictive analysis of leading indicators. Detection typically relies on cyber

threat indicator patterns. In incident response (use case 3.3) upon detecting potential cyber threats, cyber operations personnel spring into action. They initiate investigations to ascertain the nature of the threat, meticulously examining what has transpired or is currently unfolding. Through this process, they strive to identify and understand the actual threat, its characteristics, and its potential impact. Subsequently, they may execute targeted mitigating or corrective actions to address the threat effectively (The MITRE Corporation, 2012, p. 7-8).

Sharing Cyber Threat Information, use case 4 - The MITRE Corporation (2012) in their publication states that cyber decision-makers set policies dictating the types of cyber threat information to be shared with specific parties and outline how such information should be managed. These policies are crafted based on established frameworks of trust, ensuring consistency, context, and control are maintained at appropriate levels. Once formulated, these policies are put into action, facilitating the sharing of relevant cyber threat indicators and other pertinent information among authorized parties (The MITRE Corporation, 2012, p. 8).

The STIX architecture diagram in Figure 18 illustrates the core cyber threat concepts as distinct and reusable constructs, delineating their interrelationships based on their inherent meaning and content. Based on The MITRE Corporation (2012) within each main construct bubble are brief high-level listings of relevant content types, with bracketed content indicating cardinality. Connecting arrows between construct bubbles signify relationships, with content elements within the bubble at the root of the arrow being of the type represented by the bubble at the arrowhead. Detailed elaboration of all content entries within each construct is provided within the language implementation, currently manifested as an XML Schema. The architecture describes the eight core constructs: Observable, Indicator, Incident, TTP (Tactics, Techniques, and Procedures), ExploitTarget, CourseOfAction, Campaign, and ThreatActor. The detail description of the architecture and its core constructs are presented in Mitre organization's paper (The MITRE Corporation, 2012, p. 10). The detailed description of the architecture and its core constructs are presented in Mitre organization's paper.

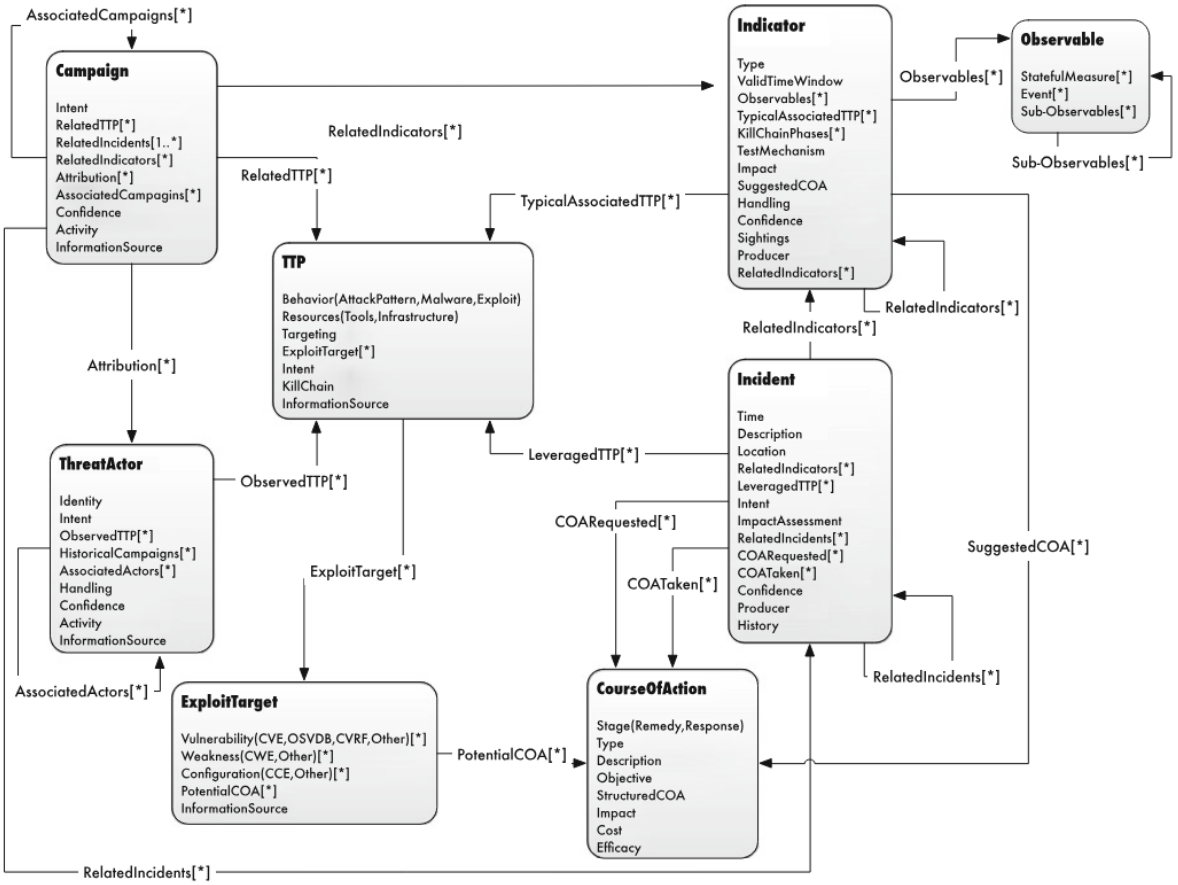

Figure 18 - Structured threat information eXpression (STIX) architecture v0.3 (The MITRE Corporation, 2012, p. 8)

7 Cybersecurity situational awareness in public sector

Studies on the current state and target state of cybersecurity within public sector organizations have been conducted by, among others, the Ministry of Finance and the National Emergency Supply Agency, taking into account aspects related to situational awareness and cooperation. Additionally, there is legislation at both national and EU levels requiring public administration and critical infrastructure organizations to ensure their cybersecurity and report cybersecurity incidents in exceptional situations. One example of this is the Network and Information Systems (NIS2) Directive, which also serves as the basis for preparing national legislation in Finland (Ministry of Justice, 2023). With the legislation introduced by the NIS2 Directive, the importance of an organization's cybersecurity situational awareness, cooperation, and information sharing can be seen to be increasing. Based on European Parliament directive the deadline for transposing the NIS2 Directive

into national law is by October 17, 2024, with the application of the directive beginning on October 18, 2024 (European Parliament, article 41.1).

NIS2 directive requires reporting to the responsible authority of any cybersecurity incident that has a significant impact on the provision of services to customers (European Parliament, article 23.1). The directive also encourages information sharing between operators subject to the directive and other entities, where such exchange aims to prevent, detect, and manage incidents, recover from them, or mitigate their effects, as well as to enhance cybersecurity levels by increasing awareness of cyber threats, limiting or preventing the spread of such threats, supporting various defense capabilities, vulnerability remediation and disclosure, threat detection, restriction and prevention techniques, mitigation strategies or management and recovery phases, or by promoting public-private cooperation in cyber threat research (European Parliament, article 29.1-29.4).

7.1 Public sector digital security statements in Finland

In 2020, the Ministry of Finance published statements for digital security in the public sector, outlining the development of digital security in public administration and thereby refining Finland's cybersecurity strategy for the public sector in 2019. It also supported the ongoing preparation and implementation of the cybersecurity strategy development program (Ministry of Finance, 2020, p. 9). The publication defines digital security as encompassing risk management, business continuity management, preparedness, cybersecurity, information security, and data protection issues (Ministry of Finance, 2020, p. 16). According to the publication, the rapid progress of digitalization, threats related to the misuse of data and misinformation, as well as increased national and international interdependence, impose new requirements for digital security across the entire public sector and its governance, laying the foundation for these statements. The guidelines are as follows.

- *We lead the security of the digital society jointly based on situation awareness and risk assessments.*
- *We manage and measure the impacts and costs of digital security in the public sector.*
- *We improve citizens' and staff understanding about the impacts of digital security risks and responsibilities.*
- *We improve digital security through public-private-people collaboration.*

- *We have an influence on EU and international digital security and utilize the outcomes of the collaboration.*
- *We require technologies and service provision to be secure* (Ministry of Finance, 2020, p. 9)

The guidelines emphasize collaboration among different stakeholders, situational awareness, risk-based management and decision-making. One key development mentioned as a digital security service supporting processes and services is the national and international collaboration model for digital security in public administration. According to the publication, through national and international cooperation, the coordination and effectiveness of digital security are enhanced, and Finland's competitiveness is promoted (Ministry of Finance, 2020, p. 14).

7.2 Public sector cybersecurity situational picture and cooperation in Finland

The Ministry of Finance published in 2022 a report on the cooperation model for digital security in public administration, aiming to describe the current state, target state, and key proposals and development needs regarding digital security in public administration. The report was based on the government's policy decision on digital security in public administration (VM 2020:23), which was implemented through the action plan for digital security in public administration 2020–2023 (Haukka). One of the tasks for founded coordination group of Haukka action plan was to produce a report on the cooperation and management model for digital security in public administration based on the preliminary investigation, laying the foundation for potential legislative preparation (Ministry of Finance, 2022, p. 9).

The study (Ministry of Finance, 2022) interviewed members of the coordinating group, consisting of representatives from public administration organizations. The interviews aimed to map the current and target state of digital security cooperation between state, welfare, and municipal sectors, as well as identify significant challenges in implementing cooperation. The interviews were conducted between October 2021 and February 2022, totaling 26 interviews (Ministry of Finance, 2022, p. 10-11). Based on the current state assessment, the study identified areas and themes of cooperation where it would be possible to harmonize cooperation management among different stakeholders. A summary of these is provided in Figure 19.

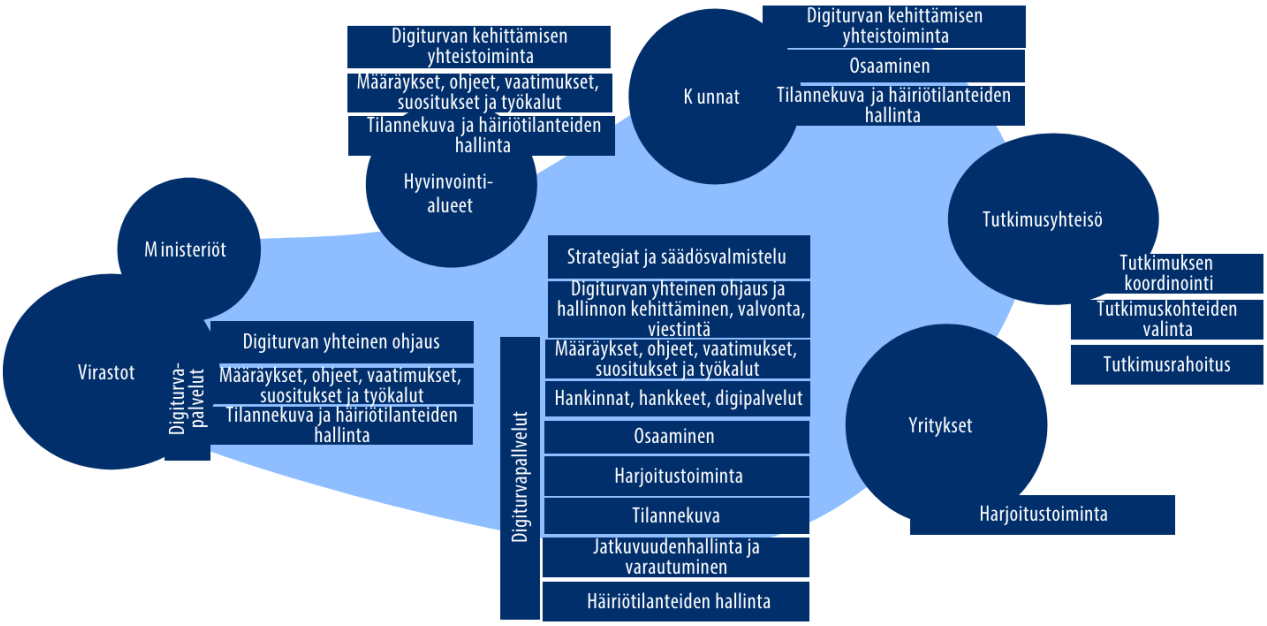

Figure 19 – Co-operation areas and themes for integration (Ministry of Finance, 2022, p. 13).

As one of the themes related to cooperation, the report (Ministry of Finance, 2022) describes situational awareness and incident management. Based on the report, DVV has maintained an administrative digital security status web service since fall 2022, where organizations report their digital security status. This service, known as the comprehensive picture service, assesses an organization's identification, description, and implementation of digital security procedures, processes, and guidelines. It covers digital security level development, resources, training, expertise, improvement areas, and risk perspectives, enabling self-monitoring and comparison with other organizations. It produces reports and monitoring data on digital security across public administration (Ministry of Finance, 2022, p. 22).

According to The Security Committee (2017) maintaining the situational awareness of the government leadership is a strategic task of the Prime Minister's Office. The Situation Center of the Prime Minister's Office provides proactive and real-time situational awareness for the government leadership to support decision-making. The task of situational awareness activities is to ensure that the government leadership has access to up-to-date and analyzed security situation awareness in all circumstances. The situational awareness is formed and updated as real-time as possible during a disturbance situation. The Situation Center of the Prime Minister's Office has the right, without

being restricted by confidentiality regulations, to obtain necessary information from the competent authority for compiling the situational awareness regarding security events. The Situation Center of the Prime Minister's Office shares a harmonized situational awareness with the President of the Republic, the Government, and other authorities. The analyzed situational awareness formed through continuous monitoring provides the basis for decision-making and crisis management. In national arrangements, cooperation with EU and international actors is utilized (The Security Committee, 2017, p. 31).

According to Ministry of Finance (2022), during incidents, the Prime Minister's Office provides a societal and information systems disruption situation picture to government leadership and authorities through cooperation. However, no overall situation picture is available about wellbeing services counties. Sharing the situation picture information is partly unclear due to some being classified or confidential. The Prime Minister's Office's digital security situation includes various national and international public and non-public sources, mostly from National Cyber Security Centre, supplemented by communities and other authorities' information. Additionally, the emergency supply organization's pools and the National Bureau of Investigation produce situation pictures related to security of supply and cybercrime, respectively (Ministry of Finance, 2022, p. 22).

Based on the report (Ministry of Finance, 2022) situation awareness information is also exchanged through Information Sharing and Analysis Centre (ISAC) groups, established to increase confidential information exchange among organizations. However, challenges exist in forming organization-specific and sector-specific situation pictures due to information collection and updating deficiencies. Limited cooperation hinders situation picture development and maintenance. The lack of a common information system solution for exchanging classified information among authorities poses a challenge (Ministry of Finance, 2022, p. 22-23).

The report (Ministry of Finance, 2022) states that situation picture compilation process lacks dialogue on threats or their effects, inhibiting the understanding of interdependencies and uniform risk management measures. Despite shortcomings, some organizations use the situation picture to inform decision-making, while in others, it remains accessible only to expert-level staff (Ministry of Finance, 2022, p. 23).

According to the Ministry of Finance (2022) report, in current state of situational awareness in the ministries and government agencies, there is a comprehensive virtual incident response Team (VIRT) existed. The VIRT group includes all ministries and some agencies, allowing for coordination of tasks and practical measures to manage disruptions. The group has two main purposes: 1) managing incidents situations and sharing situation awareness, and 2) developing cybersecurity. Additionally, the National Cyber Security Centre (NCSC) and state administration actors share situation information in the state administration's Information Sharing and Collaboration Group (ISAC) (Ministry of Finance, 2022, p. 27).

The report (Ministry of Finance, 2022) describes that in the administrative sector of the Ministry of Social Affairs and Health, in current state of situational awareness, cooperation areas are formed around university hospitals which collectively support their welfare regions in matters related to cybersecurity and security incident management. The Social Insurance Institution's control center is intended to serve as the joint security operation center (SOC) for these cooperation areas in the future. The establishment of dedicated centers within the cooperation areas is being explored. The National Cyber Security Centre (NCSC) provides guidance to actors in managing incident situations. The police investigate any potentially related cyber-related crimes (Ministry of Finance, 2022, p. 29).

Also based on the research of National emergency supply (2022), in the field, data protection controls and measures are already formally managed due to regulations, but cybersecurity requires more systematic measures for several actors (National Emergency Supply Agency, 2022, p. 15, 29). The report describes that the healthcare sector demonstrates good baseline maturity, capable of managing cybersecurity in a formalized manner with various data protection controls and quality standards. Its crucial role in enabling population health and well-being enhances its attractiveness as a target, making continuous development and improvement in cybersecurity essential. To enhance maturity level, the following recommendations are suggested by the report.

- Due to staff turnover, organizations should ensure staff understanding of their role in implementing cybersecurity.
- Expand the identification of supply chains and dependencies beyond immediate suppliers.

- Ensure comprehensive consideration of security throughout the application development process, following the DevSecOps approach (National Emergency Supply Agency, 2022, p. 29).

The Ministry of Finance's (2022) report proposes as target state in public sector level situational awareness to establish a comprehensive, proactive knowledge base and versatile metrics derived from various government agencies, wellbeing services counties, and municipalities, as well as modular reporting capabilities to support the formation of common situational awareness and understanding for decision-making. As one measure, led by the Ministry of Finance, an assessment of the technological solutions needed to create environments for handling security-classified information by authorities will be conducted. Additionally, the entire government sector faces a growing need for processing international information, and related issues need to be addressed across the entire government sector. Particularly, the NATO-produced situational awareness and its utilization must be considered. To promote information exchange within the government sector, comprehensive collaboration needs to be initiated. To achieve this, data models, interfaces, and collectively agreed-upon and defined practices and processes are required (Ministry of Finance, 2022, p. 57).

In the report (Ministry of Finance, 2022) one of the main nine target state service areas in public sector's digital security is situational awareness. The description of the service area, charged mainly for National cyber security agency, states that the goal is to provide common and shared situational awareness solutions for digital security and information security, based on extensive data, diverse metrics from across the public sector, and modular reporting to support the formation of common situational awareness and understanding for decision-making. Solutions can be supplemented or enriched with internal situational awareness data. The service area produces, maintains, and develops situational awareness data and products for public administration, based on expert analyses. This includes utilizing forecasting, organizational maturity assessments, compliance assessments of information systems, and automatic technical monitoring (Ministry of Finance, 2022, p. 67). The service area consists of the following parts.

1. Collection and compilation of data for analysis and formation of situational awareness products.
2. Distribution and publication of situational awareness data, partially provided as self-service "on-demand" solutions, and separately providing organization-specific summaries of situational awareness data for defined groups (Ministry of Finance, 2022, p. 67).

The report states that each organization is responsible for managing its internal situational awareness data. Situational awareness data is needed comprehensively from the public sector and communities (Ministry of Finance, 2022, p. 67).

8 Interview results

This chapter describes summaries for each of the interviewed organizations. Analysis of interview results was formed and identifies key findings that are utilized in development of cybersecurity situational awareness model in next chapter. All the interviews were held between 21st of May and 7th of June 2024.

8.1 Interview summaries

In total eight interviews were held for the participating organizations. For security reasons the names of the organizations are not presented nether name of the persons interviewed. The titles of the interviewees were CTO, CISO, Service Director, Service Manager, Cybersecurity specialist and Cybersecurity Business Director. The interview followed the same structure, and all the questions were the same. In the beginning introductions were made by participants and the target of the study and interview was presented. After that the definition of cybersecurity situational awareness was introduced based on the Security Committee (2018) definition. Littering was started when we moved to go through the questions.

8.1.1 Wellbeing Services County #1

According to the interviewee, in the first interviewed wellbeing services county, their organization creates a shared cybersecurity situation picture from which reports are made for different levels of groups. The content of the reports expands the higher the reporting level, but they are based on the same shared situation picture.

- **At the tactical level**, the cybersecurity situation is reported by ICT service providers to security experts.
- **At the operational level**, the cybersecurity situation is reported to the organization's IT management.
- **Strategic-level** reporting occurs annually and is reported to the organization’s management. There’s also a strategic information security and data privacy group gathering four times in a year where a situation report is made for.

On a weekly basis, the service provider produces a periodic cybersecurity situation report. The security manager interprets the situation report with their team and raises awareness of IT-related issues within the IT department as needed. If there are no issues to raise, no reporting is done. Additionally, a separate strategic group for security and privacy meets four times a year to form its own security situation report.

The organization has its process for forming a cyber situation picture, with defined responsibilities, but it is not based on any general situation awareness model, standard, or framework. The organization also has an ICT asset management solution that supports vulnerability management and related risk assessment.

Regarding the direction of cyber situation awareness, the information security manager provides requirements to their team for forming the cybersecurity situation picture, such as what things to monitor and focus on. The team's experts decide how monitoring and data collection are implemented. They have access to security products and technologies that provide a comprehensive view of the organization's ICT environment, including its systems, versions, servers, network devices, and endpoints. With these, they can identify vulnerabilities related to the environment's IT assets. Additionally, they scan their IP addresses from the outside to detect any open ports or services. The organization also conducts audits of selected information systems or collections of systems. Regarding the external operating environment, the organization monitors the national and global cyber operating environment, especially regarding threat actors and vulnerabilities. A challenge mentioned by the interviewee is the formation of a cybersecurity situation picture for SaaS services, but a solution is being sought to monitor SaaS service vulnerabilities using their own products in the future.

The organization uses antivirus, XDR, SIEM, and SOAR systems to obtain information about their environment's cybersecurity situation. Additionally, they have specialized products to restrict program execution. Email security solutions also provide information about the environment's security. The data collection and processing are considered challenging because information must be obtained from multiple ICT-provider’s business areas to form the situation picture. There are many

data sources and needs, so combining them is laborious, which can hinder the formation of a coherent situation picture. Challenges are particularly mentioned regarding situation awareness information from SaaS services.

Regarding visualization, information is always presented from a broader perspective the more strategic the reporting level, for example, using images or simple statistical views. At the tactical and operational levels, the presentation varies depending on the situation and audience. There is no standardized model or technique in use for presenting the situation picture. Security products provide a wealth of information about the environment, such as numerical data and automatic assessments. This applies only to the ICT assets managed by the organization, but reporting capabilities for SaaS services cannot yet be extended, so a comprehensive situation picture cannot currently be built.

At the tactical level, the environment is constantly monitored, and daily decisions are made that are not visible to end-users and do not require funding. If decisions require funding based on situation picture information, for which the security manager's budget or authority is not sufficient, the decision is made by the IT department at the operational level. At the strategic level, decisions are made that have long-lasting or broad effects and that can affect many the organization's employees.

The organization's cybersecurity situation picture is not shared with others, but for example if a vulnerability in a medical device is identified, the information can be shared with other wellbeing services counties or partner organizations through the Sote-ISAC group or by direct cooperation. There are also preparedness centers in the social and healthcare sector for cyber-attack situations, and situation information is shared through these centers with other organizations in the sector.

Regarding situation awareness information shared by others, they only use situation picture information distributed by the National Cyber Security Centre. The Sote-ISAC group operates internally within the sector, and at the national level, they are part of a national ISAC group, enabling international cooperation through the National Cyber Security Centre. Additionally, they are involved in the ICT service provider's cybersecurity customer group and will establish a development group

for the cybersecurity of wellbeing services counties nearby soon. Experts can also use informal channels to gather information as part of the cybersecurity situation picture.

Regarding national guidance, the definition of cybersecurity situation awareness is perceived as unclear. If multiple wellbeing services counties should provide their cyber situation pictures to the Ministry of Social Affairs and Health, each would do it in their own way. Clear common guidance is needed to determine what the cyber situation picture means, how it is collected, what information it contains, and how it is shared.

Regarding overall security, the organization actively monitors national and international security situations. For example, when Russia attacked Ukraine, they kept track Russian actions more closely. This is done by following recommendations and communications from Finnish authorities and taking into account potential issues affecting them in their situation picture. The interviewee also mentioned that currently, they do not receive threat information from anyone about potential actors and their motives, indicating potential attack intentions against them. This information is collected within the organization to the best of their ability but without national-level resources and understanding.

Finally, the interviewee mentioned that because there is no mandatory requirement for the social and healthcare sector to produce a cybersecurity situation awareness according to a specified model, the National Cyber Security Centre forms an incorrect situation picture of the sector's cybersecurity situation. Some organizations in the sector provide information to the National Cyber Security Centre as they see fit, but some of them do not. The National Cyber Security Centre should define the methods, parameters, and ways for forming and distributing the situation picture for the sector, making the information standardized and automated across different organizations.

8.1.2 Wellbeing Services County #2

In the second wellbeing services county, according to the interviewee cyber situational awareness reporting can be categorized into three levels in their organization: strategic, tactical, and operational. This hierarchical structure ensures that cybersecurity information is communicated effectively across various levels of the organization. At the operational level, the cybersecurity situation

picture is formed mainly using Security Operations Center (SOC) functions, external network analyses, and vulnerability management. The information gathered at this level is provided to the organization's security manager, who then disseminates it to the IT management team. The operational level focuses on the technical details and immediate security issues that require prompt attention and action.

The tactical level focuses on the state of ICT services and their agreed security service levels. The cyber situation picture at this level helps in monitoring and managing the performance and compliance of ICT services with security requirements. Reporting at this level is done quarterly, and it involves more higher-level assessments compared to the operational level.

The strategic level involves minimal monitoring and reporting, which has been identified as a current shortfall. The management does not demand or provide guidance for cybersecurity situation reporting at this level. As a result, critical information from the lower levels is selectively brought to the attention of the management. Currently, the formation and reporting of the cyber situation primarily remains at the operational and tactical levels. Reports are created during service management meetings, where security issues can be added to the agenda. The reporting frequencies are as follows.

- Operational Level: Weekly reports
- Tactical Level: Quarterly reports
- Strategic Level: Annually, as part of the ICT annual report

The organization lacks a formalized model for creating the cybersecurity situation picture. Current practices have evolved based on needs, but there is a recognized necessity to define and document the process. The absence of a comprehensive security management model contributes to this gap. Related to the data sources of internal environment, the data is collected from ICT devices and software using various security products and services. Information is also gathered through change management, vulnerability assessments, identity management, SOC services, and cloud services. In an external environment information is sought from service providers and their security practices, including contract compliance. Technical monitoring of the external network is

conducted, and social media channels are monitored for reputational risks. Industry, national, and international security trends are also tracked, albeit with inadequate tools.

Currently, the security manager guides the process and information collection for cyber situational awareness. As this role is assigned to only one person this creates a key person risk. The reliance on a single individual for guidance and analysis underscores the need for a documented and systematic approach to forming the cyber situation picture.

Specific technologies used were not described in detail, but Shodan is mentioned as a valuable tool. Information from data exchange groups and service providers is also utilized. Data from various sources ultimately goes to the security manager, who performs the analysis and forms conclusions. These are then discussed with service providers and higher organizational leadership as necessary. These practices are informal and lack a documented process.

Related to the decision-making process at an operational level the decisions are related to technical controls, such as software approvals, endpoint decisions, and firewall rules. In tactical level the decisions are related to service providers and contract compliance, including security requirements for procurements. Security training decisions are also often made at the tactical level. In strategic level minimal reporting leads to few decisions at this level.

In information sharing, a national social and healthcare Information Sharing and Analysis Centre (Sote-ISAC) is the key information exchange channel where the member organizations share their cyber situation pictures. Information includes as an example security findings and new threats. The National Cybersecurity Centre's communication tool is utilized for sharing the situation picture of ongoing security incidents as an example. In reginal level there are unformal smaller groups of 2-3 wellbeing services counties to share more detailed information. Cyber situation information is shared with their service providers too to help them understand the customer's environment better, though this is not a regular action. In international level, there is not currently any cooperation group that the organization belong to.

Related to the challenges and development areas for formation of cybersecurity situational awareness, one key improvement area is automation. Improving automation for real-time data collection and presentation is seen as a key development area for situational awareness. Continuous external assessments could provide a current view of the attack surface, keeping the organization informed in real-time about the situation.

Another issue mentioned is management engagement. Educating the management on using the cyber situation picture as a management tool is seen crucial. In the patient context, situation information is used in their organization well to identify available beds relative to patients and staff as an example. Similarly, cybersecurity situation information should be utilized at the management level.

In information sharing the member organizations often hesitate to share extensive information about their cyber security situation that is seen as an issue. Enhancing cooperation and trust among member organizations is essential for comprehensive information sharing.

The organization is developing a broader security situation picture, with cybersecurity being one part. A security coordination group meets monthly, including representatives from risk management, security, information security, preparedness, and occupational safety, with plans to add an environmental security representative to the group in future. This group reviews all aspects of overall security and gathers once a month.

As a conclusion the current practices in cybersecurity situation reporting within the organization highlight significant strengths and areas for improvement. Formalizing and documenting the process, improving automation, and increasing leadership engagement are critical steps towards a more effective and comprehensive cybersecurity posture in their organization.

8.1.3 Wellbeing Services County #3

Cybersecurity situational awareness in this Wellbeing Services County is monitored and reported at both the operational and strategic levels, but not at the tactical level, according to interviewee. At the operational level, the cyber environment is monitored daily, and a weekly situational report is discussed in the operational security group. These reports cover observations, incidents, and

global cybersecurity events. At the strategic level, a strategic security and data protection group meets quarterly, including representatives from the organization's leadership. These meetings track the progress of cybersecurity initiatives, global trends, and phenomena, and their relevance to the organization.

Major cybersecurity events are reported separately at agreed intervals and methods, potentially even to the board level if necessary. The formation of cybersecurity situational awareness is part of the service provider's SOC operations, and the situational awareness is reported as part of the purchased SOC service, which gathers information from systems like SIEM. Information from various collaborative groups is also integrated. Although there are established practices for the overall process of forming situational awareness, areas for improvement have been identified.

The process is primarily guided by the organization's security manager, considering the needs of the data protection officer. The management does not set requirements for data collection or metrics for situational awareness. Internally, the functionality of security controls, such as firewalls and antivirus systems, as well as the installation of updates and service providers' SLA levels, are monitored. Externally, the status of partner networks and cybersecurity announcements from authorities are followed. Situational data is also gathered from collaborative groups such as Sote-ISAC and the Ministry of Social Affairs and Health's cybersecurity group, and other collaboration groups. Situational awareness data is collected using security products and technologies, such as antivirus solutions, firewalls, software inventory systems, network traffic analysis tools, SIEM solutions, and usage monitoring products. Some national communication systems are also used for sharing information with stakeholders.

At the operational level, situational reports are provided by service providers and SIEM systems. For the strategic level, information is compiled from various sources, and analyses and reports are manually crafted into an understandable format for the leadership. For visualizing the situational awareness, the reporting features of security products are used, without additional visualization systems.

Decisions based on situational awareness are discussed in the operational weekly meeting. Decision-making at the operational level depends on the asset being protected, and the decision is often made by the asset owner. At the strategic level, decisions focus on major development projects and significant changes. Changes are implemented through the change management process, but there are no specific models for tracking or measuring security-related decisions otherwise.

The overall cybersecurity situational awareness is not shared externally, but essential information can be shared within certain collaborative groups. The organization utilizes cybersecurity situational awareness information produced by others, such as service provider reports and weekly reports from the National Cyber Security Centre. Cybersecurity collaboration is conducted in groups coordinated by the National Cyber Security Centre, such as Sote-ISAC, the national cybersecurity group coordinated by the Ministry of Social Affairs and Health, and in some less formal regional wellbeing services counties groups, as well as with certain authorities. Although opportunities for international collaboration have been identified, it is not currently undertaken.

The main area for improvement in forming cybersecurity situational awareness is the understanding of the organization's cyber environment. This is based on IT asset registry and enterprise architecture data, which help identify dependencies and assess the impact of security events. Enterprise architecture is seen as particularly important for forming situational awareness and evaluating the impacts of events. Other areas for development include refining external environmental information into the organization's cyber situational awareness and addressing data protection issues between the EU and other countries.

The organization has its own guidance for organization security, which includes cybersecurity as one aspect. Currently, cybersecurity and data protection have been integrated into a unified function, strengthening joint reporting and operations.

8.1.4 Wellbeing Services County #4

The Fourth wellbeing services county organization reports cybersecurity situational awareness through a three-tiered approach. At the operational level, situational awareness is reported monthly during meetings with the service provider. The organization's internal cybersecurity and

data protection team operates at this level. At the tactical level, there is a steering group for cybersecurity and data protection that also monitors situational awareness on a monthly basis. This group includes representatives from various units of the organization. At the strategic level, there is no regular meeting practice for reporting cybersecurity situational awareness; instead, this information is communicated as needed, such as in the case of a significant cybersecurity incident that impacts the entire organization. The organization has recognized the need to develop strategic level reporting practices, particularly considering the national implementation of the NIS2 directive. Cybersecurity is integrated into their overall risk management process, and they produce monthly cybersecurity situational awareness reports for the relevant group.

The organization does not have a documented formal process for creating and reporting cybersecurity situational awareness. However, they are currently undertaking development measures to improve this area. The guidance for forming cybersecurity situational awareness primarily comes from the tactical level steering group for cybersecurity and data protection. The Chief Information Security Officer presents proposals to this group, which then makes decisions.

For the internal environment, cybersecurity situational awareness data is derived from SOC service reports, service level information, and data on specific monitored issues such as identity login data, which helps define security regulations for the organization's environment. Currently, vulnerability information is focused on external network scans, and employee-reported security incidents are also part of the internal situational awareness data.

For the external environment, global cybersecurity trends are monitored. Additionally, information is obtained from stakeholders such as service providers, contractual partners, and collaboration groups like Sote-ISAC. They are also adopting the National Cybersecurity Center's observation service.

The technologies and security services used by the organization are concentrated among a few service providers. Solutions mentioned include SIEM and cloud platform security technologies. At the operational level, analysis and action proposals come from their SOC service provider. They also have a practice of reviewing cybersecurity incident topics in workshops, which form the basis for action decisions to improve security. There are no specific analysis or visualization tools for the

tactical and strategic levels. For visualization, an interviewee mentioned the service produced by Digital and Population Data Services Agency (DVV), which provides graphical insights into their cybersecurity maturity through periodic assessments, useful for presenting situational awareness.

Decisions based on cybersecurity situational awareness at the strategic level have broad implications for the organization or the responsibilities of officials, such as policy decisions related to cybersecurity. At the tactical level, decisions involve risk management measures or security methods. At the operational level, decisions are less impactful on personnel and are related to production or employee guidance. The organization follows up on the impact and implementation of decisions on a case-by-case basis without a formal model or process. For important measures, monitoring methods can be agreed upon in periodic cybersecurity and data protection team or steering group meetings.

Cybersecurity situational awareness is shared with the organization's stakeholders, particularly the regional preparedness center, partners, and information exchange groups, with Sote-ISAC mentioned in the interview. The organization also utilizes the situational awareness information from these channels in its operations and threat impact assessments. International collaboration is limited to participation in the Sote-ISAC group coordinated by the National Cybersecurity Center, which brings in necessary information from international ISAC groups.

The organization lacks a clearly documented framework for forming cybersecurity situational awareness, which is recognized as a current challenge. This is, however, being developed. Another challenge mentioned is clarifying and documenting responsibilities, which can affect decision-making. A third challenge is their broad cybersecurity environment and limited resources to secure it.

8.1.5 Government Agency #1

In the first government agency the formation of the organization's cybersecurity situational awareness is structured in three levels: operational, tactical, and strategic. At the operational level, the organization's IT infrastructure and its security are monitored on a daily basis. The primary audience for these reports includes service managers and IT specialists within the organization. Situational awareness is reported every two weeks during the service production meeting. Daily vulnerability monitoring is also performed, and any findings are reported to their vulnerability

information channel on a daily basis. Additionally, product teams within the organization hold their own meetings where security-related observations and incidents are reported. Regular operational-level meetings are also conducted with service providers to discuss the state of cybersecurity.

At the tactical level, cybersecurity situational reporting is conducted for the organization's IT management. This reporting occurs in a monthly meeting attended by IT management representatives and product group managers.

At the strategic level, the organization's Chief Security Officer (CSO) reports on the cybersecurity situation to the Chief Executive Officer (CEO) or the executive management team. The interviewees did not provide specific details about the reporting frequency at this level. Strategic reporting is also conducted for the supervising ministry upon request. There are dedicated collaboration groups for cybersecurity managers and IT managers within the specific administrative sector, which also receive updates on the organization's cybersecurity situational awareness.

The organization has also a separate security group that includes representatives from various security domains in addition to the cybersecurity service manager. The CSO manages this group, and cybersecurity matters are reported to the group weekly.

The organization currently lacks a clearly documented process for forming its cybersecurity situational awareness. Instead, practices have evolved based on needs. However, they are actively developing the process for tactical-level cybersecurity situational reporting. At present, some of the information for cybersecurity situational awareness is obtained through automation from various systems, but the compilation of data from these sources involves a significant amount of manual work.

At the strategic level, the guidance for forming cybersecurity situational awareness comes from the CEO through the CSO, who oversees the entire security domain. The CSO conveys the needs and high-level goals to the IT management, which then directs the formation of situational awareness at the tactical and operational levels.

Regarding the internal operational environment, the information gathered for cybersecurity situational awareness includes data from firewalls, SIEM solutions, SOC services, vulnerability management systems, and other monitoring systems. Additionally, at the operational level, security incidents and breaches reported and detected are included in the situational reports.

For the external operational environment, essential information is collected from stakeholders' reports, such as vulnerability releases or weekly National cybersecurity center's situation reports. Other key sources of external information include the VAHTI working groups coordinated by the Digital and Population Data Services Agency (DVV), cooperation groups with service providers, and media reports or news. At the strategic level, ministries can also provide situational information in various scenarios, which is utilized to form the organization's situational awareness. However, the monitoring of the external operational environment is less intensive compared to the internal environment.

The practices for integrating, refining, and reporting cybersecurity situational information are currently informal. The information is compiled and analyzed in the best possible way in current state and reported in various ways. This work is mostly manual. The organization does not currently have dedicated tools or technologies for visualizing cybersecurity situational awareness; instead, reporting and visualization rely on general office applications. Visualization related to ticket counts can be obtained from ITSM systems, and similar visualizations can be derived from SOC services. The goal is to implement a reporting system in the future that can better visualize cybersecurity-related information.

Operational-level decision-making relates to actions such as mitigation actions for incidents, decisions to correct deviations, and measures for identified vulnerabilities. If a significant security incident occurs, there is a specific process for reporting the situation to the management if necessary. At the tactical level, decision-making focuses on risk management. Strategic-level decisions pertain to broader development measures and their funding, with the IT management also being involved. Currently, the organization does not have tools or metrics to measure the impact of decisions. The only recognized measure was the monitoring of vulnerability remediation.

Cybersecurity situational awareness information is not shared comprehensively within the organization, except with ministries or in meetings of cybersecurity managers within the administrative sector. At the strategic level, the information shared is very general. In tactical-level collaboration meetings with suppliers, events related to their operations are discussed. In DVV's coordinated collaboration meetings, situational information is reported as needed in a limited manner.

The organization utilizes cybersecurity situational information received from its stakeholders to understand its own environment. The key sources include meetings with suppliers, central meetings with ministries and agencies, and other previously mentioned networks. Other cybersecurity-related collaboration groups include earlier mentioned meetings coordinated by ministries, administrative sector groups meetings, meetings with suppliers, and state administration network meetings. There are also general cooperation groups in which the organization participates, where cybersecurity is one of the topics discussed as needed. No international cybersecurity groups were identified.

The interviewees mentioned limited expertise and resources as the main challenges in forming their cybersecurity situational awareness. The organization has recognized the need to improve its security culture and many cybersecurity-related processes require more definition and documentation. Due to resource constraints, prioritization is often necessary. From a technical perspective, the organization needs more real-time visibility tools for the cyber environment and tools to proactively detect threats. A system like MISP threat sharing platform was mentioned as a technological need.

Another key challenge identified was the classification of cybersecurity situational information and how it can be handled in different environments and the limitations for sharing it with others. As described in the theory section of this thesis, this is known as a common problem based on the studies.

8.1.6 Government Agency #2

In the second government organization, a dedicated service for situational awareness is part of the security and risk management function. The service manager is responsible for creating security situational awareness and managing security incident process. The organization's situational

awareness encompasses not only information security but also personnel security, and facility security. Situational awareness is developed at strategic, tactical, and operational levels, refining the collected information into a precise situational picture, which is further condensed for higher-level reporting.

Operational status is monitored daily and compiled into a weekly situational picture. Tactical situational awareness is created monthly and reported to various management groups, such as monthly product group meetings. It covers cross-sectional security issues within the organization. At the strategic level, situational awareness is also compiled monthly and reported to the organization's top management. This strategic report includes an overview of the operational environment, predictive situational awareness, and significant issues impacting the entire organization or its core functions. Although reporting is tiered, the terms operational, tactical, and strategic are not explicitly used; these are internal practices for security situation reporting. Key points from each situational picture are progressively highlighted and escalated, with a focus on forecasting. The organization has evaluated the necessity for semi-annual security reviews, but this practice has not yet been implemented.

The organization does not have an officially defined process for creating cybersecurity situational awareness, but it is produced in a process-like manner. Information gathering activities are process-oriented with agreed reporting practices for reviewing the cyber situational picture. There are clearly defined roles, functions, and meeting practices for monitoring and guiding security situational awareness. Additionally, they have a security management IT system where security incidents are processed, and reporting views are compiled within the same system.

Guidance for creating the situational picture primarily comes from a designated organizational-level security situational awareness service manager. This person develops models and processes for situational awareness creation. Guidance and requirements are also gathered through discussions with other units and relevant stakeholders within the organization. Furthermore, security leadership provides needs and questions to be addressed in the situational awareness report. The responsibility for creating the situational picture rests with the service manager. Higher management provides guidance and needs for situational awareness formation only as needed, such as

during significant security events that might affect the whole organization. Situational awareness is created in close collaboration with other security area managers.

Related to information sources and analysis, in the internal environment the cybersecurity situational picture is formed from observations by the security operations center, malicious email detections, and vulnerability management findings. Besides cybersecurity observations, the security situational picture includes personnel security incidents, staff-reported security events, and facility security incidents. In an external environment the organization actively collaborates with various authorities, integrating their information into its security situational picture. They also receive structured threat information and reports from stakeholders. Threat data is also gathered and intelligent using their own methods and systems.

Multiple technologies are employed for information collection, although specific tools and technologies were not mentioned in the interview. Their security IT management system is central for data collection, with integrations established from other security and ICT environment systems. Collected data is analyzed in operational-level meetings using monitoring views and metrics from security systems. These analyses result in reports presented to different groups at various levels. The organization has predefined visualization views for monitoring current security status and trends. Their security IT management system includes the primary visualization solution. Additionally, a separate visualization system with predefined security metrics is available for top management. At operational and tactical levels, situational awareness can be reviewed without qualitative analysis based on observations. For strategic level reporting, the information must be qualitatively analyzed and evaluated.

In operational level the decision-making involves resolving identified security incidents, advancing situations, and implementing necessary follow-up and improvement measures. At the tactical level the decisions often pertain to identified security phenomena affecting multiple organizational actors, requiring communication to the staff. Decisions are also made regarding risk management and security service levels. In strategic level the decisions involve broader security improvement measures and their financing, with IT management also participating.

Security-related decisions are monitored for effectiveness through risk management, such as reducing risk levels with implemented controls. Monitoring methods depends on the specific decision. If a particular phenomenon or event is identified for monitoring, its progress is tracked in agreed meetings. However, there is no formal process for tracking decision impact beyond the mentioned methods. In significant incident situations, a retrospective meeting is held post-event to review the incident and the success of the situational awareness process. This serves as feedback for improving the situational awareness process.

The organization shares their security situational awareness with key stakeholders and utilizes their provided information. For instance, they collaborate with the National Cybersecurity Centre. They participate in security-related cooperation groups and engage in bilateral discussions with individual partners about the security situation. Generally, their collaboration is goal-oriented and systematic. Cybersecurity situational awareness information from partners is refined and compared with their observations, aiding in predictive situational awareness. In general, collaboration occurs within the sector, bilaterally, in networks, or as part of larger cooperation groups. International cooperation is based on sector level collaboration.

In forming cybersecurity situational awareness and picture, one mentioned significant challenge is integrating external environmental information and assessing its impact, although the organization has managed this reasonably well. Another challenge involves barriers to sharing threat information between the authorities. It is suggested that threat information from various security authorities should be more accessible to civilian authorities as they form a major part of the national preparedness and secures availability of critical national services. Legal and information classification issues, and in some cases cooperations network limitations, hinder this.

The third major challenge mentioned is limited financial resources, especially given the current budgetary constraints in government administration. The organization’s overall security includes information security, personnel security, and facility security. Cybersecurity is part of information security, and its situational picture is reported at different levels. The security function also monitors existing information influence activities and hybrid operations.

As conclusion, the organization presents a higher level of maturity in cybersecurity situational awareness compared to other interviewed organizations. The already existed teams and roles dedicated to security situational awareness including tools and systematic cooperation practices highlight this.

8.1.7 ICT Service Provider #1

The first ICT service provider organization develops and produces digital services for the social and healthcare sector and for government agencies. The organization reports its cybersecurity situational awareness at three levels. Cybersecurity reports are submitted to the organization's top management and board twice a year, and additionally upon request if the management wishes to monitor significant cybersecurity phenomena or events more closely. In the tactical level cybersecurity situational awareness is monitored biweekly during security working hours, addressing issues related to cybersecurity development and task prioritization. The group includes the Chief Information Security Officer (CISO), the Chief Technology Officer (CTO), and the Chief Architect.

At the operational level cyber situational awareness is reported weekly, focusing on daily events such as incidents detected by the Security Operations Center (SOC). The CISO is responsible for creating the situational picture, and various reports are tailored to the respective target groups. The organization does not have a formally defined process for situational awareness; practices have evolved based on needs and existing capabilities. A mentioned challenge is compiling a comprehensive security overview of the digital services produced by the organization, for which new operational models are being implemented.

Guidance for creating the cybersecurity situational picture primarily comes from the tactical level through the CTO and CISO. The CEO may also provide requirements and questions guiding situational awareness formation, typically related to general security conditions or specific cybersecurity incidents within the industry that might impact the organization. Information collection from internal environment focuses on data from the SOC service, status information of services produced by other organizational units, risk and threat assessments, results from security audits, including security tests and maturity assessment results. From external environment the information is gathered from service providers, the National Cybersecurity Centre, social media, and news sources.

The SOC service, Security Information and Event Management (SIEM) solutions, risk mappings, ICT platform security monitoring systems, and vulnerability management systems are the primary information sources. Information is compiled from multiple sources, some of which provide detailed reports. These are consolidated into cyber situational reports, highlighting the current state of the cyber environment, how the situation has evolved, and where problems have been identified. The final report creation is a manual process, with higher-level summaries produced for top management. Currently, there are no separate systems or solutions for visualizing cybersecurity situational awareness; general office applications are used for this purpose.

Related to strategic decision-making, based on situational awareness, major development project decisions are made, often involving significant investments. In tactical level the decisions relate to development plans and actions that do not require substantial funding. At the operational level smaller changes and corrective actions for deviations are decided. In sudden critical incidents, operational decisions can also be significant. There is a separate architecture group in the organization that makes technology related decisions. Units developing and producing digital services have significant decision-making power regarding cybersecurity implementation, but the cybersecurity function sets the principles and provides recommendations for solutions. Monitoring of decisions impact focuses on risk management and the implementation of risk mitigation measures. There is no specific formal process for tracking the impact of decisions beyond this.

The organization does not currently share its cybersecurity situational awareness information with other stakeholders but utilizes information produced by others. Information is sought particularly from the National Cybersecurity Centre's bulletins and reports. Additionally, the organization participates in national VAHTI groups and organizes an annual digital security customer day.

Limited resources and information overload are cited as the main challenges in forming cybersecurity situational awareness. With information coming from various sources, the challenge is to identify relevant information specific to the organization.

The organization does not see the need for a separate comprehensive security situational awareness or a dedicated group for it, as their security-related activities are not extensive. However, there are designated individuals responsible for risk management and facility security.

8.1.8 ICT Service Provider #2

The second ICT service provider organization provides a wide range of ICT services, including cybersecurity services for their social and healthcare and other public sector customers. The interviewed person represents the management of their cybersecurity services. The organization reports on the cybersecurity environment to its customers and internally. Reporting is conducted both at the operational and tactical levels regularly for customers. Strategic level reporting is done only upon the customer's request. The operational cybersecurity situational picture includes information compiled from technical systems and external sources and is reported weekly. Tactical level reporting is conducted monthly. The organization is also implementing a Security Orchestration, Automation, and Response (SOAR) solution that allows customers to independently view information about their cybersecurity environment.

Currently, there is no formally described process for forming cybersecurity situational awareness; it is based on established practices and customer needs. However, the organization has identified the need to define and describe this process as they are developing the preparedness centers functions for their customers, where forming a situational picture is essential.

Guidance for creating the cybersecurity situational picture primarily comes from customer needs but can also arise from national collaboration groups and public administration organizations. Customer needs and subsequent guidance for forming the situational picture are discussed in periodic collaboration meetings.

The situational picture for the internal environment consists of data collected from multiple customer environments, numbering several dozen. Information is primarily gathered using SIEM and SOAR systems, as well as other technical security systems. From external environment the information is collected from authorities’ bulletins, collaboration group meetings, service providers, and media. The organization also purchases situational reviews on cybersecurity from an external company, produced on a weekly, monthly, quarterly, and annual basis.

According to the interviewee, understanding the customer's environment and industry is crucial for analyzing the impact of detected events and phenomena. The organization compiles cyberse-

curity situational reports and recommendations, but the actual conclusions are made by the customer. If the situational data reveals areas for improvement, recommendations are included in the reports. Strategic level reports also include conclusions. Currently, the organization does not use separate visualization tools for presenting the cybersecurity situational picture but utilizes general office applications. The implemented SOAR solution will offer operational level visualization views for customers in the future.

In strategic level the decisions made based on the cyber situational picture are often related to security evaluations and audits, and actions derived from their results. In a tactical level plan for the actions are decided to achieve strategic objectives. Operational level decisions are related to implementation of the planned actions. Decisions impact assessment and monitoring focus on the achievement of strategic goals and the implementation of risk management measures.

The organization shares its cyber situational information with customers within its trusted network. If a cybersecurity event occurs with one customer, related information can be shared with other customers without disclosing the affected customer's identity. Additionally, information related to situational awareness is shared in National Cybersecurity Centre collaboration groups. The organization often participates in industry-related cyber exercises, practicing, for example, the use of the MISP system. They have a nationally coordinated channel for sharing event information between SOC centers, but its usage is currently not very active. Collaboration is also conducted with public administration organizations in the industry. The organization is also involved in VAHTI networks and the National Emergency Supply Agency's collaboration groups.

The main challenges in forming cybersecurity situational awareness are the availability of senior-level expertise and collaboration between SOC operations. Recruiting high-level, experienced cybersecurity professionals is currently challenging. Situational awareness could be improved if different organizations' security operation centers shared more information about their observations and situational awareness. Competitive dynamics are seen as a challenge, but a national authority like the National Cybersecurity Centre could act as a central contact point and coordinator. The organization has also identified the need to define and describe the process for forming cybersecurity situational awareness as a development area.

The organization has a preparedness group that compiles a comprehensive security situational picture, of which cybersecurity situational information is a part. Similarly, their customers have preparedness centers where cybersecurity is one key aspect of overall situational awareness.

8.2 Analysis for the interviews

This analysis synthesizes insights from eight interviews with different organizations regarding their approaches to forming cybersecurity situational awareness and their comprehensive security posture. The organizations discussed include wellbeing services counties, government agencies, and ICT service providers. The analysis identifies similarities and differences in their approaches, highlights best practices, and suggests areas for improvement.

Most of the interviewed organizations implement a hierarchical reporting structure, encompassing operational, tactical, and strategic levels even though in all organizations these exact hierarchical terms are not used formally. This ensures that cybersecurity information is communicated across various levels of the organization, albeit with different frequencies and depths of detail. As an example, wellbeing services counties #1 and #2 utilize weekly operational reports, quarterly tactical reports, and annual strategic reports. None of the organizations addresses a technical level cyber situational awareness reporting as described in some of the theories. The most common and process-oriented level for cyber situational awareness reporting seems to be daily and weekly basis monitored operational level and tactical and, in some organizations, strategical levels are not so well defined.

None of the interviewed organizations has a formal documented process that addresses all the three mentioned reporting levels for cybersecurity situational awareness. Some organizations though have identified this as a developmental action. There is a significant variance in how formalized and documented the processes for forming situational awareness are. Wellbeing services county #1 and Government agency #2 have somewhat formalized processes with defined responsibilities, though they lack adherence to a general model or framework as presented in theory section of this thesis. Wellbeing services county #2 lacks a formalized model, relying heavily on the security manager, which presents a key person risk. The lack of formal process was seen to affect decision-making, especially at a strategical level where the reporting practices were more infor-

mal. Another conclusion was that CSA data was collected from several sources and combined usually in manual way. The formal documented process could enhance the data collection, fusion and analysis. The technical capabilities had some differentiation between organizations that also affected the performance of CSA formation.

The degree of leadership engagement in cybersecurity situational awareness varies. Some organizations have proactive leadership and require cybersecurity situation reporting, while others indicate minimal involvement. As an example, wellbeing services county #3 indicates a lack of strategic-level leadership requirements for data collection and metrics. In many cases the CISO is the one who is directing the data collection and gathers the needs from different stakeholders. ICT Service Provider #1 and Government agency #2 reports that cybersecurity awareness is periodically reviewed by top management and the board, demonstrating higher engagement.

Organizations gather situational awareness data from both internal and external sources. As an example, Wellbeing services counties #1 and #2 collect data from various internal security products and external sources such as service provider reports and national advisories. Internal data includes information from firewalls, antivirus systems, SIEM solutions and other technical capabilities. External data encompasses threat intelligence from national sources, service providers, and industry trends. Data collection from internal environment is more mature than collecting information from external environment. External environment data collection is in many cases based on personnels own activity for following media and other open sources. Some mentioned issues related to external environment data collection are information overload and lack of formal tools for external data collection and analysis.

The reliance on SOC functions for forming the cybersecurity situation picture is prevalent. SOCs and the tools they use e.g. SIEM, SOAR and XDR solutions, provide essential services such as continuous monitoring, incident response, and vulnerability management for all the interviewed organizations. This is emphasized as an example by wellbeing services county #3 and ICT provider #1. Most of the organizations form a single detail cyber situational picture at the operational level that is compressed and summarized into higher level decision-making groups.

The use of automation in data collection and situational awareness reporting is uneven across organizations. Wellbeing services county #2 recognizes the need for improved automation for real-time data collection and presentation. ICT Service Provider #1 emphasizes the role of SOCs and automation in maintaining up-to-date situational awareness. They also are deploying a self-service portal through SOAR solution for their customers. Automation is utilized in internal operational environment using SIEM, XDR and SOAR systems for data collection but automation is needed more to collect and gather other internal source and external source data. In general, a need for a more comprehensive cybersecurity situational awareness system that automates the data collection, analysis and reporting can be seen needed based on the interviews as there is still lots of manual work in the process.

Many organizations collaborate with National cybersecurity Centre and are part of their coordinated Information Sharing and Analysis Centers (ISACs) to enhance and limitedly share their situational awareness information. These collaborations help in sharing threat intelligence and best practices. Wellbeing services counties and some ICT providers engage with Sote-ISAC and the National Cyber Security Centre for information sharing and collaboration. Government Agencies also participate in ISACs and benefit from national-level cybersecurity insights. The cooperation is done point-to-point collaboration between individuals, within the sector level of their industry, in national groups and in some cases at the international level. Cybersecurity situational awareness information is collected also from public events and conferences.

In conclusion, while organizations show a commendable effort in forming cybersecurity situational awareness, there are notable differences in their approaches. Addressing the highlighted areas for improvement can lead to more effective and comprehensive cybersecurity postures across the board. Here are the key findings from the interviews.

- There is a clear need for formalized and standardized processes across all organizations to enhance the consistency and reliability of cybersecurity situational awareness. National authorities' guidelines could help in defining clear methods and parameters for situational awareness reporting and information sharing. This could also support building a higher accurate national level cybersecurity situational picture.

- Increasing leadership engagement at all levels is critical. Educating leaders on the importance of cybersecurity situational awareness as a management tool can improve strategic decision-making and resource allocation.
- In forming cybersecurity situational awareness, a comprehensive IT asset management inventory and knowledge of organizations enterprise architecture is crucial for assessment and projection of cybersecurity events.
- Investing in automation for real-time data collection and presentation can significantly enhance the accuracy and timeliness of situational awareness. This can help in proactive threat detection and response. Cybersecurity situational awareness is established by various technical systems and external reports. In its current state, this process requires extensive manual work to combine these sources, perform analysis, and generate reports. This highlights a need for comprehensive cybersecurity situational awareness system.
- Utilizing advanced visualization tools and standardized models for presenting situational awareness data can improve understanding and communication across all levels of the organization. This includes integrating capabilities to monitor SaaS services and external environments comprehensively.
- Encouraging more extensive information sharing within national and international collaboration groups can provide a more comprehensive cybersecurity situational picture. Enhancing trust and cooperation among member organizations of different cooperation groups is essential for this.

8.3 Developed model for cybersecurity situational awareness

This thesis proposes a comprehensive model for the formation of cybersecurity situational awareness (CSA) within an organization. The model integrates technical capabilities and sources, a detailed cybersecurity situational awareness process, and robust mechanisms for information sharing and cooperation. The goal is to provide a structured approach to enhancing an organization's ability to detect, analyze, and respond to cybersecurity threats effectively.

As stated in the theoretical section of this thesis, cybersecurity situational awareness is crucial for organizations to protect against increasingly sophisticated cyber threats. This model outlines the

components and processes necessary to develop an effective CSA system, ensuring timely and accurate information flow from detection to decision-making and action. The target for developing the model was to visualize the into one figure to see the full picture of the elements related to formation of CSA. The detailed model is described in Figure 20.

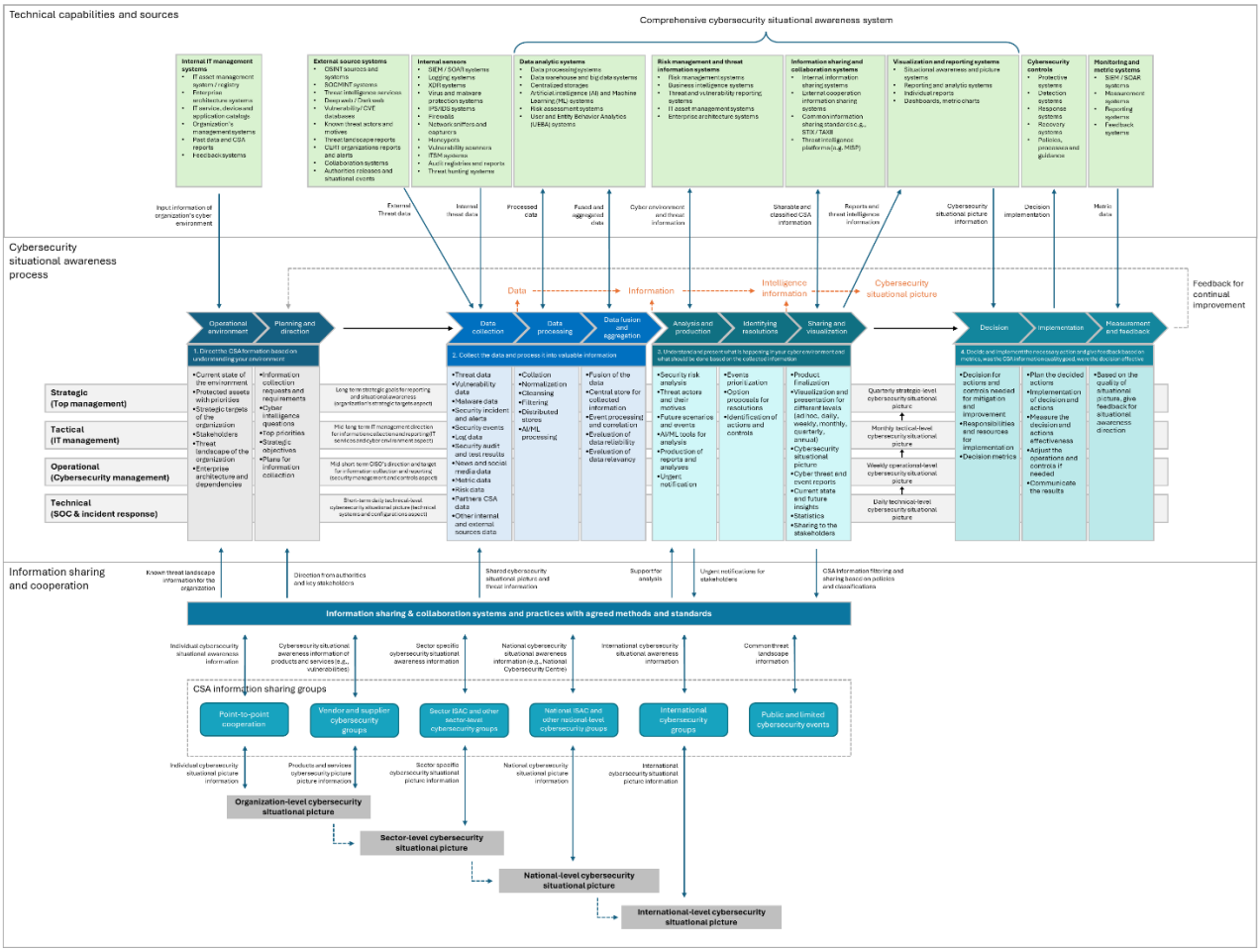

Figure 20 - Developed comprehensive model for cybersecurity situational awareness (CSA)

The objective of the described model is to provide a concrete vision with sufficient precision so that various organizations can benefit from it as broadly as possible. The model is not intended to be followed in its entirety; rather, the idea is to allow organizations to extract and apply the elements relevant to them. Therefore, the model should be adapted to the organization's specific context and operational environment. The model was developed by integrating phases and contents from several previously described theories and combining them with the findings and conclusions from the interview phase. The model illustrates the interdependencies of different layers,

how technological capabilities and information sources relate to various phases of the process, and at which stage in the process cybersecurity situational awareness information is exchanged.

In the model's technology layer, there is a designated area that reflects the technological components of a system dedicated to cybersecurity situational awareness. This information is not based on previous research but represents the author's perspective on the critical components of such a system. By integrating these components, it would be possible to achieve a centralized system for data collection, processing, integration, analysis, visualization, and information sharing. This perspective also forms one of the key topics for further research. The phases of the different layers of the model are described in more detail in the following subsections.

8.3.1 Cybersecurity Situational Awareness Process

The CSA process is an iterative cycle encompassing several stages, ensuring a structured flow from data collection to actionable decisions and continuous improvement. This model proposes the main areas and steps to form the cybersecurity situational picture and to make and measure the decision related to cyber environment events. The model describes also who data is transformed into intelligence information, marked as organge text, based on the Borges Amaro, Percilio Azevedo et al. (2022) theory introduced in the chapter 5.1 of this paper. The main process includes steps from the Endsley's model, CCOP model, multi-level analysis framework for CSA and cyber threat intelligence life cycle. This theory information has been riched from the results of the interview held for the public sector organizations. The process developed is visualized in Figure 21.

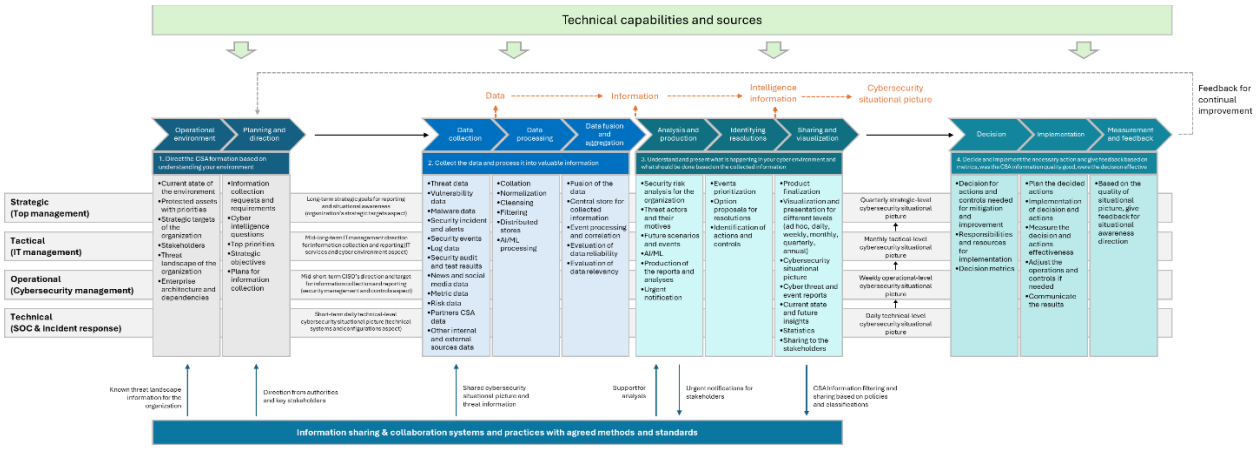

Figure 21 - Process of developed CSA model

The process Figure highlights that there are four main levels of formation of cuybersecurity situational picture. The directon and planning is also done in these level. In chapter 8.3.4 is describe examples of the content of situational awareness picture and what kind of decisions are made in these organizationa decision-making levels.

The four main areas of this process are (1) directing the CSA formation based on the understating the organization's environment, (2) collecting the data and processing it into valuable information, (3) understanding and presenting what is happening in the organization's cyber environment and what should be done based on the collected information and finally (4) decide and implement the necessary actions and give feedback based on the metrics, was the CSA information quality good enough and were the decision effective. These four main areas are divided into process steps as follows:

- **Operational Environment**: This stage involves creating a comprehension of the organization's operational environment and current state. Understanding the current cyber security environment and identifying the system dependencies are critical when planning the CSA information collection and targets for the situational picture content. Operational needs of stakeholders are analyzed to inform the subsequent planning and direction phases. Key activities include the identification of critical assets, maintaining an inventory of IT and cybersecurity resources, understanding the threat landscape and enterprise architecture.
- **Planning and Direction**: The aim for this stage is to form clear goals and plans for forming the cybersecurity situational picture with correct content with precise detail. Strategic planning involves defining long-term goals for CSA and allocating resources accordingly by top management. Organizational objectives are integrated into the CSA planning, ensuring alignment with overall business goals. The stated information collection requests and requirements are formatted into cyber intelligence questions and prioritized at the tactical level. Detail plans are created for data collection and processing at an operational level. In technical level the plans for configurations for internal and external sensors are created. The planning and direction stage also establishes clear roles and responsibilities for managing CSA.
- **Data Collection:** Data is collected from various sources, both internal and external. This includes real-time monitoring data, historical data, and information from threat intelligence

feeds. Effective data collection forms the backbone of the CSA process. Key data sources include SOC services, network logs, endpoint security events, application security logs, and external threat intelligence including OSINT feeds. The integration of data from these diverse sources ensures comprehensive visibility into the security environment. In the process step description in Figure 21, there are listed some examples of beneficial to data collect.

- **Data Processing**: Collected data undergoes normalization and enrichment to ensure consistency. Filtering, cleaning and correlating events help in making sense of the vast amounts of data. The key is to format the data into a useful format and filter the valid data for the next stages. Techniques such as the application of machine learning algorithms are employed to enhance the accuracy and reliability of threat detection data. In this stage the data may be stored into severe stores where data can be retrieved into centralized storage in the next phase.
- **Data Fusion and Aggregation**: Aggregated data provides a holistic view of the security landscape. Centralized storage allows for easy access and better data management. Prioritizing data based on relevance and risk ensures focus on the most critical threats. The use of data warehouses and big data platforms enables the efficient storage and retrieval of large volumes of security data, supporting advanced analytics and reporting in next phases. As the data is fused, the evaluation of data reliability and relevancy is made to ensure high quality base for analysis and production.
- **Analysis and Production**: At this point the data is formatted to valuable information and centralized for analysis. Comprehensive information analysis is crucial for accurate threat detection and assessment. The analysis phase aims to understand and assess security risks. Actionable intelligence is generated, and detailed security incident reports are produced for further action. Security risk analysis involves the identification of threats, vulnerabilities, and potential impacts, along with the development of mitigation strategies. In addition to understanding the current situation of the cyber environment, the projection of future scenarios is crucial. The generation of alerts and notifications for relevant stakeholders ensures that they are informed promptly about critical incidents and events they should be aware of. The products can be detail or high-level reports depending on the audience for the questions stated in direction phase or a comprehensive cybersecurity situational picture to understand the big picture of the current cyber environment state and possible future scenarios.

- **Identifying Resolutions:** The analyzed events and threats are prioritized based on their potential impact to the organization and likelihood of occurrence. Before the results are shared for decision-making, the option and proposals for resolutions of events and threats are made. By this the decision-makers understand what can be done and what are the effects in each scenario. As result the decision-makers have analyzed the picture of cyber environment with proposals for actions and controls.
- **Sharing and Visualization**: Effective communication of CSA information is vital. This stage involves finalizing the products, sharing information across organizational levels and visualizing the analyzed information through dashboards and reports. Maintaining updated situational awareness dashboards ensures ongoing vigilance. In target stage the cybersecurity situational picture information should be as real-time as possible. Visualization tools provide interactive and real-time representations of the security posture, enabling quick identification of trends and anomalies. In addition, regular reports and briefings ensure that senior management and key stakeholders are kept informed of the security situation. When it comes to information sharing, it is crucial to recognize the classification level of the information and share it only with those who have the agreed-upon right to handle classified information. Information sharing should be based on a well-defined information-sharing policy, established practices, and the use of secure information-sharing tools. This ensures that information is disseminated appropriately and securely to authorized individuals only.
- **Decision**: Informed decision-making is based on the analyzed information, proposals and intelligence. Decision-makers use cyber situational awareness insights to prioritize actions, allocate resources, and implement response plans. It is crucial to define the responsibilities and resources for the decided actions. Decision effectiveness metric and monitoring practices should define to ensure that threats are mitigated.
- **Implementation**: Response strategies and actions are implemented to address identified threats and events. The plans are made for implementation and the effectiveness of the decided controls and actions are monitored by the defined metrics. The possible adjustment for strategies and actions should be made if the threat or event cannot be mitigated. As the end results are achieved these should be communicated to the decision-makers.
- **Measurement and Feedback**: This final stage involves measuring the quality of CSA and giving feedback to the CSA direction. The evaluation of the quality of CSA information

should be made to provide feedback for the CSA direction and process owner. Regular reviews and audits of the CSA processes ensure that improvements are made based on lessons learned from past incidents. Adjustments should be made to the process and practices based on feedback, ensuring that the CSA system evolves, and the quality of products improves continuously. Performance metrics can be used to evaluate the success of the implemented strategies. Key performance indicators (KPIs) and metrics, such as incident response times, threat detection rates, and the effectiveness of mitigation measures, can be utilized to track and analyze to drive continuous improvement.

8.3.2 Technical Capabilities and Sources

Technological capabilities are essential for forming a comprehensive cybersecurity situational awareness. This model outlines the types of information systems, platforms, applications, technological solutions, and data sources involved in different stages of the process and describes the kind of information that can be integrated into the cyber situational awareness process. The combined listed information in the figure for each process phase is based on the acquired knowledge from theories and interviews introduced in this thesis. The technological aspect of the model is described in Figure 22.

During the research, information was gathered on the technologies organizations use for collecting, analyzing, and visualizing cyber situational awareness data. The findings revealed that there is no clear, comprehensive system dedicated to forming cybersecurity situational awareness; instead, information is collected and processed across multiple systems, in many cases mainly from operational level detection systems. This model also proposes a framework for what a comprehensive cybersecurity situational awareness system might encompass.

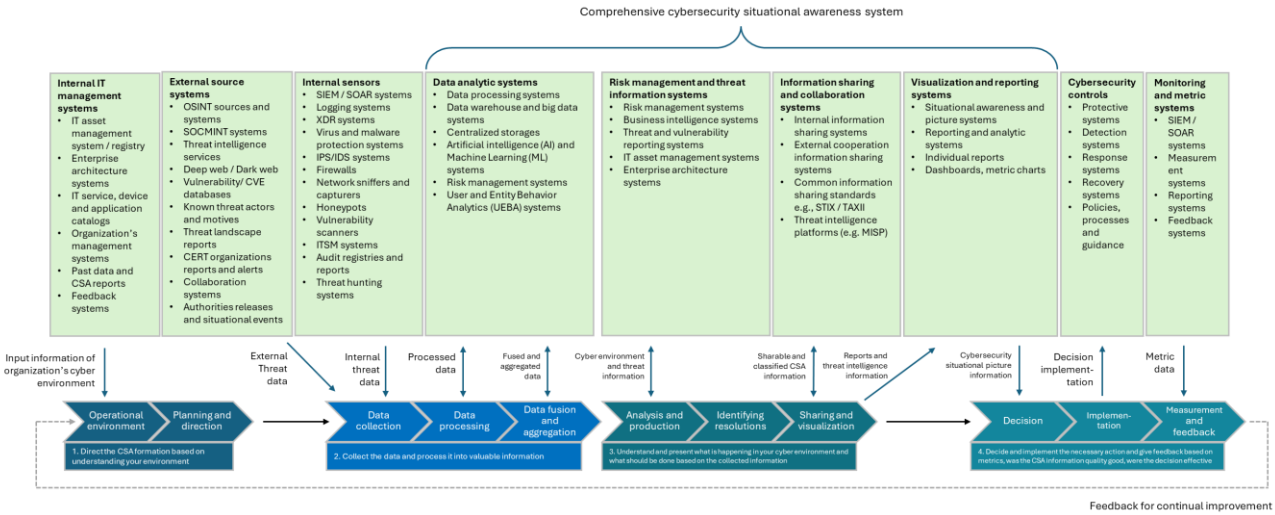

Figure 22 - Technical capabilities and sources of the developed CSA model

The foundation of the CSA system lies in the diverse range of technical capabilities and sources utilized for data collection and threat detection. The technologies and sources related to the process steps are described as follows.

Internal IT Management Systems: Organizations must manage their internal assets through robust IT asset management and registry systems. These systems should work in tandem with endpoint protection, firewalls, IDS/IPS, and comprehensive network systems to provide a comprehensive view of the secure IT infrastructure and data. The inclusion of enterprise architecture systems ensures that the organization functional services, data, systems and technologies are known including their dependencies ja prioritizes. This is crucial for understanding the threat landscape and gives direction for planning data collection related to cybersecurity situational awareness. The past CSA reports and feedback from earlier CSA cycles are utilized in understanding the operational environment.

External Source Systems: Threat intelligence is gathered from various external sources such as open-source intelligence (OSINT), threat intelligence feeds, vulnerability databases, social media monitoring, CERT/CSIRT reports, and security advisories. These external insights are crucial for staying updated on the latest threats and vulnerabilities. Key element in this phase is to collect data from collaboration tools and cooperative stakeholder groups.

Internal Sensors: Within the organization, internal sensors play a pivotal role. Network and SIEM (Security Information and Event Management) systems, alongside endpoint detection and response (EDR) tools, monitor activities in real-time. Application security systems, identity and access management (IAM) systems, and cloud security solutions also contribute to a comprehensive internal security posture. Moreover, advanced persistent threat (APT) detection systems and anomaly detection tools are employed to identify sophisticated and stealthy threats that might evade traditional security measures. The deployment of deception technologies and the use of threat hunting practices further enhance the organization's ability to detect and respond to emerging threats. In context of internal operational environment, audit reports and partner reports related to internal environment can be utilized.

Data Analytics Platforms: Advanced data analytics systems, including SIEM and machine learning-based systems functionalities, process large volumes of security data. These platforms utilize big data analytics and user and entity behavior analytics (UEBA) to identify patterns and anomalies that might indicate a security threat. The integration of artificial intelligence (AI) and machine learning algorithms enables the automation of threat detection and the prediction of potential security incidents.

Risk Management and Threat Assessment Systems: To understand and mitigate risks, organizations employ risk management systems and threat modeling. These systems help in compliance management and vulnerability assessment, which are essential for proactive cybersecurity measures. The use of quantitative risk assessment tools allows for a detailed evaluation of potential impacts and the prioritization of risk mitigation efforts. Internal IT asset management and enterprise architecture systems should be utilized for assessing the impact and dependencies of found threats.

Information Sharing and Cooperation Systems: Effective cybersecurity situational awareness relies heavily on information sharing. Threat intelligence platforms and collaborative data exchange systems e.g., Open Source MISP enable organizations to share critical information about threats and vulnerabilities internally and externally. Information sharing agreements (ISA) and standardized protocols, such as STIX/TAXII, facilitate the secure exchange of threat intelligence between organizations and across sectors.

Visualization and Reporting Systems: To make informed decisions, data needs to be visualized effectively. Management dashboards and advanced analytics systems provide clear, concise views of security metrics. Additionally, the implementation of interactive visualizations and real-time reporting capabilities ensures that decision-makers have access to up-to-date and actionable information. The detailed content of the visualized cybersecurity situation picture relies heavily on the needs and requirements of decision-makers and operational environment.

Cybersecurity Controls: In implementation of decided actions multiple security protective, detective and response system can be utilized depending on the nature of the decision. Some mitigation actions may include updating or creating new policies, processes and guidance for the organization. The key is to utilize the correct and effective technology to prevent proactively threats realization.

Monitoring and Detection Systems: Continuous monitoring is essential for real-time threat detection and monitoring. SIEM, SOAR (Security Orchestration, Automation, and Response) platforms, honeypots, and system logs provide comprehensive monitoring capabilities that can be utilized for measuring effectiveness of implemented actions. Feedback systems can be utilized for giving feedback was the provided CSA information valuable and good quality.

8.3.3 Information Sharing and Cooperation

The sharing and utilization of cybersecurity situational awareness information is one of the most crucial factors in forming a robust cyber operational environment. This model outlines the primary information-sharing groups identified in the research at a high level and their relationship to the creation of cyber situational awareness at various levels. The model is heavily based on the public administration perspective since the interviewed organizations represented public administration, and the theoretical section also extensively discussed public administration collaboration models.

Information sharing occurs in various ways, and the model generally describes that information exchange in both directions takes place through different collaboration and information-sharing

systems, practices, and agreed-upon methods and standards. The model illustrates the stages where collaboration is particularly necessary and specifies the type of information that is shared.

The model emphasizes that collaboration and information exchange occur through established systems and methods. It highlights that the information sharing should be done according to established information-sharing policies and considering information classification. This model does not address the stages of decision-making and feedback. Its primary focus is on the exchange of information, ensuring that it aligns with information-sharing policies and classification requirements. This approach ensures that the information is shared securely and appropriately across the relevant groups and stages of the process. The information sharing and cooperation aspect of the model is presented in Figure 23 and described in more detail in the following.

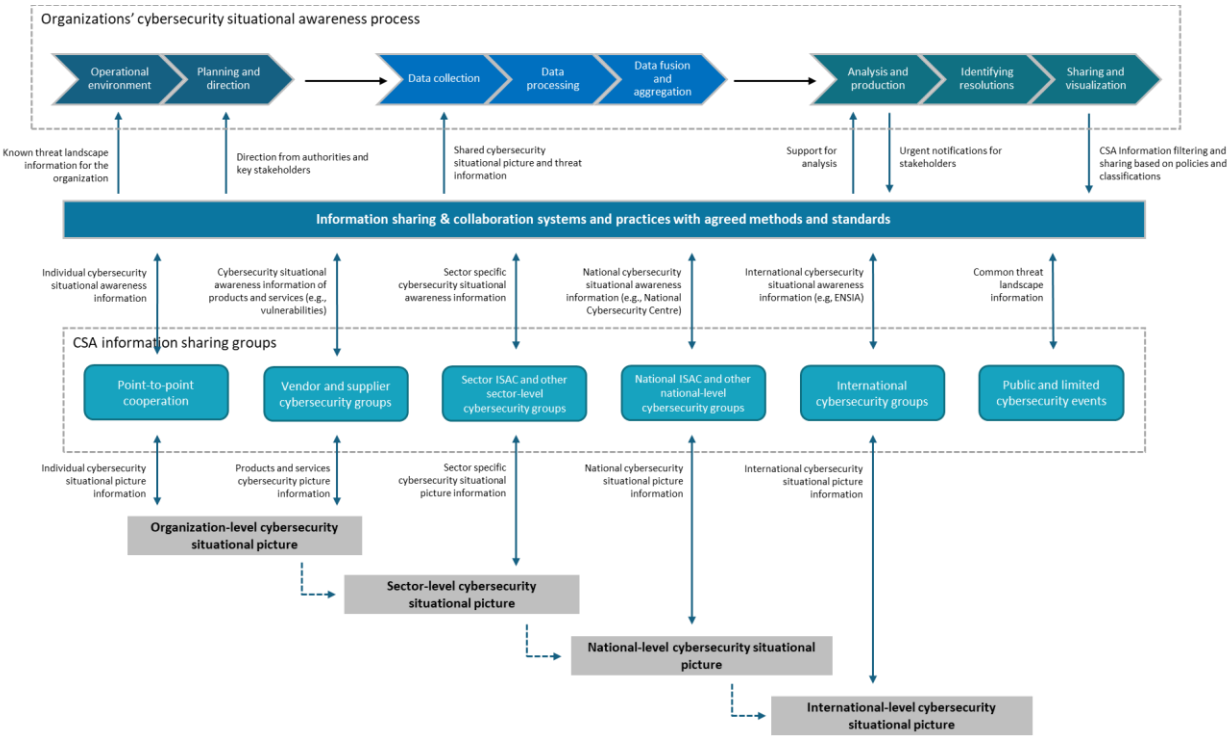

Figure 23 - Cooperation in developed CSA model

CSA Information Sharing Groups: Collaboration is facilitated through different groups or channels between different stakeholders. The identified cooperation groups for CSA information sharing are

- Point-to-point cooperation for individual information sharing. As an example, this could be communication between two wellbeing services counties or government agencies.
- Vendor and supplier cybersecurity groups for sharing information related to products and services. Usually this of communication between the customer and key ICT service provides.
- Sector-specific ISACs (Information Sharing and Analysis Centers) for sharing the CSA information related to specific sector, domain or industry. As an example, Social and Healthcare ISAC is one of these kinds of groups.
- National ISACs and groups where CSA information is shared regardless of the industry.
- International cybersecurity groups where CSA information is shared between organizations in multiple countries. This can be sector-specific or general CSA cooperation group.

These groups ensure that critical threat information is shared promptly and accurately. Participation in public cybersecurity events and forums allows organizations to stay informed about the latest trends and developments in the cybersecurity landscape. This can be also seen as an information and collaboration channel for cybersecurity situational awareness.

While planning and directing the CSA formation in the process of model, information can be acquired from stakeholders to support understanding the threat landscape of the organization or industry. Authorities may also give direction and guidance for planning the CSA information collection and analysis. In data collection shared CSA information is one of the key sources. This may include vulnerabilities, threats, occurred incidents and other relevant information found by the stakeholders. In analysis phase, stakeholders can support to understand the collected information and impacts for the organizations. They also may share the mitigation and resolutions for the threats. The organization itself may also notify its stakeholders if they find and analyze some urgent threat information. As the cybersecurity situational picture is formed, that can be shared to stakeholders based on the policy and data classification with agreed partners.

In the interview there was described that in public administration the cybersecurity situational picture is formed in sector and national level. The model describes how different cooperation groups

and information shared within those affects forming the cybersecurity situational picture in different levels. These identified levels are organization-, sector-, national- and international-level cybersecurity pictures. These are described in high level as follows:

Organizational-Level Cybersecurity Situational Picture: Within the organization, data from various departments is integrated to develop a comprehensive cybersecurity situational picture. This holistic view enables better understanding and management of internal security posture. Regular internal briefings and reports ensure that all relevant departments are aware of the current security situation and can take appropriate actions.

Sector-Level Cybersecurity Situational Picture: Sector-specific cybersecurity information is shared to address common threats and vulnerabilities related to the sector, domain or industry. Sector ISACs play a crucial role in facilitating the exchange of threat intelligence and best practices among organizations within the same industry. In these groups information from the international sector specific groups may also been shared.

National-Level Cybersecurity Situational Picture: National coordination of cybersecurity efforts involves sharing intelligence with national agencies and other organizations regardless of the sector they operate in. This collaboration enhances the overall security posture at the national level. National cybersecurity centers and coordination bodies can provide a platform and tools for the aggregation and dissemination of threat intelligence across the country.

International-Level Cybersecurity Situational Picture: Global cybersecurity initiatives benefit from international threat intelligence sharing. Collaboration on an international scale ensures that organizations are prepared to tackle global cyber threats. International cybersecurity groups and initiatives facilitate the exchange of threat intelligence, trends, and best practices across borders, helping organizations to stay ahead of emerging global threats. An example of these international groups is The European Union Agency for Cybersecurity (ENSIA) sector ISACs groups.

8.3.4 Content of the cybersecurity situation picture and the decisions

One of the key themes of this study was to identify the decision-making processes related to cybersecurity situational awareness. This goal was primarily pursued through interviews, and partially from theory sources. However, some answers remained quite high-level. The study also identified what kind of information is reported at different levels concerning cybersecurity situational awareness. This thesis presents a concept model of decision-making for cybersecurity situational picture, structured across four distinct levels: strategic, tactical, operational, and technical. Each level contributes to a comprehensive understanding of the cybersecurity environment, informing various decisions across an organization. This model highlights the interconnectedness of situational awareness and decision-making processes, emphasizing the importance of timely and accurate information sharing. Based on these findings, this model presents examples of the types of information that form situational awareness at different levels and what its content might be. The model describes the types of decisions made at different levels based on this information. Additionally, the model outlines the most common decision-making groups at four different levels: strategic, tactical, operational, and technical. It also illustrates the time frame for compiling and presenting the situational awareness at each level. Practices vary between organizations, so the model should be considered an example or a research-based view of best practices. The model also shows how situational awareness can be used to predict future events over different time horizons relative to the level of situational awareness being presented. Similarly, regarding decision-making, the model depicts how the impact and longevity of decisions change relative to the decision-making groups at various levels. The model is presented in Figure 24.

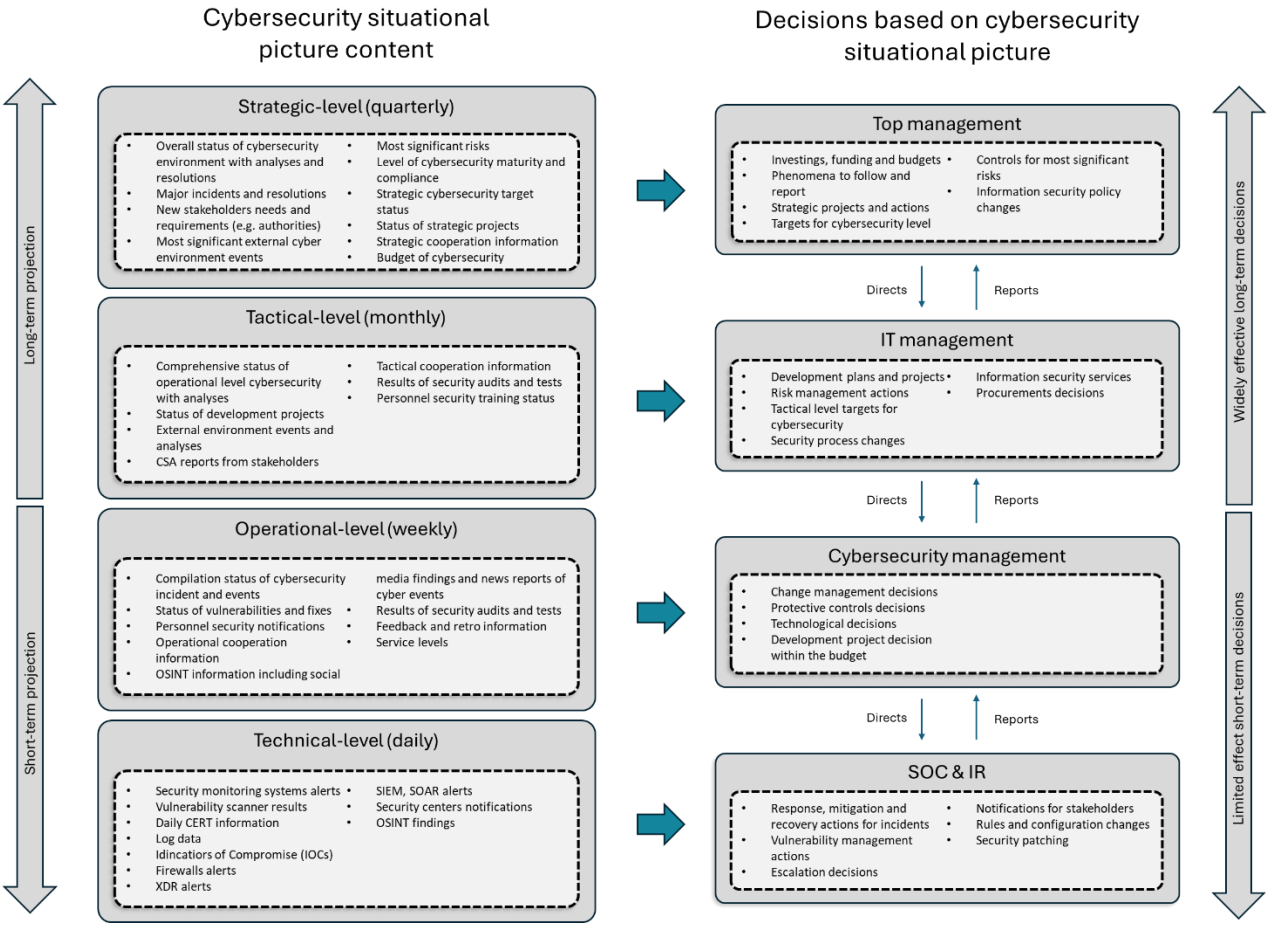

Figure 24 - Cybersecurity situational picture content and decision-making in different levels

The rapidly evolving landscape of cybersecurity threats necessitates a robust and dynamic approach to situational awareness. Effective decision-making relies on timely and accurate information that spans different organizational levels. This model delineates the flow of cybersecurity information and the corresponding decisions at the strategic, tactical, operational, and technical levels.

At the strategic level, situational awareness focuses on the overall status of the cybersecurity environment, including major incidents, stakeholder requirements, and significant external events. This level addresses long-term projections and involves high-level decisions made by top management. Reporting intervals may vary from monthly insight to annual reports. Some examples identified for content of the cybersecurity situational picture at this level includes overall cybersecurity status with analyses and resolutions, major incidents and resolutions, new stakeholder needs and requirements, significant external cyber events and most significant risks. The decisions are usually

widely effective for the organization and long-term including investment related. As an example, the decisions include investments, decisions of strategic projects and actions, setting cybersecurity targets and changing information security policies.

The tactical level involves a more detailed and frequent analysis of cybersecurity status, focusing on medium-term planning and coordination. Usually, this level is reported monthly for IT management which uses this information to make decisions that bridge strategic goals with operational needs. The content of cybersecurity situational picture may include Comprehensive status of operational-level cybersecurity with analyses development project statuses, external environment events and analyses, tactical cooperation information and results of security audits and tests. The decision may be related to risk management actions, tactical targets for cybersecurity, security process changes and procurements as an example.

Operational-level situational awareness focuses on the ongoing and short-term cybersecurity activities within the organization. This level compiles data from various sources to inform decisions by cybersecurity management, ensuring responsive and adaptive measures are in place. The most common reporting interval based on the interview is weekly basis. The content of operational cybersecurity situational picture may include compilation status of cybersecurity incidents and events, status of vulnerabilities and fixes, personnel security notifications, OSINT (Open-Source Intelligence) information, including social media findings and security service levels status. The decision is usually short term and doesn't require more funding than is reserved in CISO's budget. These decisions maybe for example change management decisions, protective controls decisions, technological decisions and smaller development project decisions within the budget.

The technical level is concerned with the immediate and detailed data collection and analysis of cybersecurity events. SOC (Security Operations Center) and IR (Incident Response) teams handle this information to provide quick and effective responses to emerging threats. The situation can be presented in daily standups and decisions are usually very short term. The content of technical level cybersecurity situational picture can include security monitoring systems alerts vulnerability scanner results, daily CERT (Computer Emergency Response Team) information, log data, Indicators of Compromise (IOCs), firewalls alerts, XDR (Extended Detection and Response) alerts, SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and

Response) alerts, security centers notifications and OSINT findings. Decisions made in this level are usually related to incident response or configuration changes. As an example, these might be related to Response, mitigation, and recovery actions for incidents vulnerability management actions, escalation, notifications for stakeholders, rules and configuration changes and security patching.

8.3.5 Conclusion

The proposed CSA model offers a comprehensive framework for organizations to enhance their cybersecurity posture. By leveraging advanced technical capabilities, structured processes, and robust information sharing mechanisms, organizations can achieve effective situational awareness and improve their response to cyber threats. The model's iterative process ensures continuous improvement, allowing organizations to adapt to the ever-evolving cybersecurity landscape. The content of cybersecurity situation picture may vary highly in different level depending on the organization and its operational environment but the model gives some found best practices to utilize in forming the organization comprehensive situational awareness capability.

9 Conclusion

The research investigated how cybersecurity situational awareness is formed based on theoretical knowledge and its practical implementation in public administration organizations. The study also explored decision-making processes at various organizational levels based on situational awareness. Although the levels of situational awareness formation varied slightly between organizations, a three-tiered model, commonly found in theoretical sources, was generally used. A key aspect of the research was to understand the collaboration and information sharing involved in forming cybersecurity situational awareness. Valuable insights, particularly from interview results, were obtained.

The first research question focused on the stages and typical content of cybersecurity situational awareness. The theoretical foundation allowed for the identification and description of the definition of cybersecurity situational awareness. Several models or processes for forming situational awareness were found in theoretical materials. Despite minor differences, these existing process descriptions followed a largely similar pattern, providing a solid foundation for the model developed in the research. Interview results also supported the development of situational awareness formation, providing detailed information on the levels and content of situational awareness. Overall, the research provided a comprehensive answer to this question, realized through the process descriptions of the developed model, presented in section 8.3.1. The research concluded that forming cybersecurity situational awareness involves guiding the formation process, data collection and processing, analysis, drawing conclusions, and visualizing the situational awareness into an understandable form for decision-makers. Continuous improvement methods, including feedback on the quality of situational awareness and the impact of decisions on earlier process stages, are also crucial.

The second research question addressed decision-making based on situational awareness. Answers were primarily sought through interviews, which provided general examples of the types of decisions made at different levels based on situational awareness. The conclusions drawn are described in section 8.3.4, which outlines the levels of cybersecurity situational awareness, their content, the corresponding decision-making groups, and the decision topics. This description, compiled from interview and theoretical data, serves as an example. Although the interview answers

were general, sufficient information was gathered to answer this research question, and the results are visualized in the description presented in the relevant section. The research indicated that decision-making could be divided into four levels, with the impact and longevity of decisions increasing at higher levels.

The third research question focused on collaboration and information sharing related to cybersecurity situational awareness. Answers were initially sought from theoretical knowledge, which discussed the benefits and challenges of information sharing, the structure of information systems targeted for sharing, and related standards. The theory section also addressed information sharing from the perspective of public administration organizations, providing a good foundation for the interviews. The interviews gathered substantial information on the key collaboration groups for these organizations, where cybersecurity situational awareness information was shared between individual organizations, within the sector, and at the national level. Limited international collaboration meant that comprehensive data on relevant groups was not obtained. Further investigation could have been conducted if national-level actors, such as ministries or the cybersecurity center, were included in the interview groups. The research visualized the collaboration groups and their connection to the situational awareness formation process and the composition of different levels of cybersecurity situational awareness in the description presented in section 8.3.3. The research indicated that collaboration occurs at various levels, involving different groups, and there are some national-level tools for information sharing. It was also found that collaboration could be improved through national regulation and clearer guidance from authorities.

In summary, the research provided well-structured answers to the research questions, which were concretized and visualized in the developed model for cybersecurity situational awareness. The result could have been even more accurate if there were more and different kinds of organizations to interview. In the end, the scope of the work had to be limited to meet the requirements of a master's thesis. Including more interviewees could have made the study too extensive. However, the research also identified several topics for further study, which could support a more detailed examination of the areas covered in this thesis.

10 Discussion

Despite the existence of general theoretical models for forming cybersecurity situational awareness, none of the organizations have utilized these models in their development efforts. This suggests that these models are either not well-known or the topic of situational awareness formation has not yet been elevated to significant importance within these organizations. However, the importance of this topic is highlighted by the fact that in one government organization, which exhibited a higher maturity level, a dedicated team and service manager were appointed for situational awareness formation. The technologies used for collecting situational awareness data are heavily focused on the operational level, and no clear tactical or strategic level situational awareness products or systems were identified during the study.

The objectives of the thesis were achieved. Based on the collected theoretical and interview data, a comprehensive model for forming cybersecurity situational awareness was developed. The theoretical material was extensive and allowed for the identification of relevant existing processes and methods for situational awareness formation. The interviews provided comprehensive information on various aspects of situational awareness formation. Although more detailed information on decision-making could have been sought, the interviews still provided general insights.

The developed model could have been more detailed and clearer if it had been tested or evaluated by existing organizations. The number of interviewed organizations could have been larger, but given the scope of the thesis, the selected number of participants was sufficient to achieve the objectives. Interviews could have also been conducted with national-level organizations responsible for forming cybersecurity situational awareness, such as the Prime Minister's Office and the National Cyber Security Center, to gain more precise information on the current state and development needs of collaboration.

The interviews also provided added value to the participating organizations, as many respondents identified gaps and areas for improvement in their own activities. Some interviewees also indicated their intention to use the model developed in this thesis to describe their own processes. The research succeeded in identifying national-level development areas related to the formation of cybersecurity situational awareness, which will hopefully be recognized by public administration.

Criticism may be directed at the literature search methods and the limitations associated with the standards and frameworks utilized. Theoretical insight could have been even wider but the founded existing models for cybersecurity situational awareness were useful. The search methods employed might have overlooked a significant amount of valuable information. Implementing a more systematic approach could potentially yield more precise and comprehensive sources.

Another criticism area is the application of model developed. As this study target was to develop the model for cybersecurity situational awareness, it hasn't been yet tested in a real-life organization context. This is one of the further research suggestions.

10.1 Reliability

The study followed the planned process for information data acquisition and model development. The information and data collected for the model was based on previous research and real-life experiments from the interviews. All the findings from the interviews are based on the interviewee's opinions and observations from their organization's perspective. The model combines multiple theoretical information that has been introduced in chapters 4, 5,6 and 7 and information from interviews described in chapter 8.

10.2 Ethicality

This study describes in detail the utilized research methods and processes, collected data, and results. References and citations adhere to APA 7 guidelines and the Ethical Principles of JAMK University of Applied Sciences (2018) to ensure proper attribution and prevent plagiarism. No personal information was gathered from interview participants, and their involvement was entirely voluntary, based on their willingness to contribute time and insights to the research. No compensation was provided to participants, and informed consent was obtained prior to their participation in any research activities. The research was done without any employer and all the participant organizations were recruited by the author. The findings were reported to the organization that participated in this study.

10.3 Further research

This study focused on researching a comprehensive process for forming a cybersecurity situational picture including the needed technical capabilities, cooperation and decision-making. The topic was quite wide, but this was a known decision. This gives a possibility for multiple further research topics. Here are listed some identified further research topics.

- This thesis work introduces a proposal for cybersecurity situational awareness model that combines information for existing research and model including the information gathered from the interviews. This model has not been applied in a real organization. This would be an interesting topic for further research.
- One of the key findings from the interview was lack of automation in cybersecurity situational awareness. Investigating the benefits and challenges of implementing advanced automation tools for real-time data collection, analysis and reporting in aspect of internal and external data sources could be beneficial. This research could explore how automation can reduce the manual workload, enhance threat detection, and improve decision-making and information sharing. A study could focus on the concept of comprehensive cybersecurity situational awareness system utilizing AI and ML tools.
- Research for analyzing the importance and impact of formalizing cybersecurity situational awareness processes within organizations. This research could compare organizations with formalized processes against those without, to identify best practices and potential pitfalls. This study could also address the needed resources and technical capabilities for higher maturity in cybersecurity situational awareness.
- Research for external environment data collection. As external environment data collection and analyses is seen as an issue for some interviewed organizations, research for investigating methodologies for improving the collection and analysis of external cybersecurity data could be useful. This could include studying the role of threat intelligence platforms, open sources, and national advisories in enhancing situational awareness.
- Research focusing on CSA collaboration and information sharing. This thesis work opened the current concepts and practices for cooperation in the public sector at a high level. A more detail research could examine the benefits and barriers to cybersecurity information sharing among organizations. This research could explore the role of national cybersecurity centers, ISACs, and other collaborative frameworks in improving collective cybersecurity

postures. The research could examine how CSA information is shared at strategic, tactical and operational levels.

- Cybersecurity situational awareness in government agencies vs. private sector. This research could compare the approaches and effectiveness of cybersecurity situational awareness in government agencies versus private sector organizations. This research could highlight unique challenges and best practices in each sector and address the information sharing practices.

References

Abu, M. S., Selamat, S. M., Ariffin, A. & Yusof R. *Cyber Threat Intelligence – Issue and Challenges.* Indonesian Journal of Electrical Engineering and Computer Science, Vol. 10, No. 1, April 2018, pp. 371-379.

Ainslie, S., Thompson, D., Maynard, S. & Ahmad, A. (2023). *Cyber-threat intelligence for security decision-making: A review and research agenda for practice*. Computers & Security, Volume 132, 2023.

Borges Amaro, L. J., Percilio Azevedo, B. W., Lopes de Mendonca, F. L., Giozza, W. F., Albuquerque, R., García Villalba, L. J. *Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data.* Applied Sciences. 2022; 12(3):1205.

Chrismon, D., Rusk, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating*. MWR InfoSecurity.

Datta, P., Lodinger N., Namin, A. S. & Jones, K. S. (2020). *Cyber-Attack Consequence Prediction.* Texas Tech University, Department of Computer Science.

Endsley, M. R. (1995). *Toward a theory of situation awareness in dynamic systems. Human Factors*: The Journal of the Human Factors and Ergonomics Society, 37(1), pp. 32—64.

Endsly, M. R. (1990). *Situation awareness in dynamic human decision making: theory and measurement.* University of Southern California.

European Parliament. (2022). *Directive (EU) 2022/2555 of the European parliament and of the council*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

Hautamäki, J. & Kokkonen, T. (2019). Model for Cyber Security Information Sharing in Healthcare Sector. 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, 1-5. IEEE.

Hedeman, E. (2022), *Cyber Situational Awareness at the Prime Minister's Office*. Laurea University of Applied Sciences.

Hirsijärvi, S. & Hurme, H. (2011). *Tutkimushaastattelu*. Gaudeamus Helsinki University Press.

Jäärni, C., Rita, M. (2024). *Helsingin tietomurrossa vuotanut arkaluontoisia tietoja – koskee jopa 120 000:ta oppijaa, huoltajaa ja kaupungin työntekijää*. Retrieved from https://yle.fi/a/74-20088356

Jiang, l., Jayatilaka, A., Nasim M., Grobler, M., Zahedi, M. & Babar, A. (2022*). Systematic Literature Review on Cyber Situational Awareness Visualizations*. IEEE Access, vol. 10, pp. 1-1.

Joukanen, T. (2023). *Miksi Venäjä aloitti hybridioperaation itärajalla vasta marraskuussa? Asiantuntija vastaa*. Yle news. Retrieved from https://yle.fi/a/74-20062916

Kananen, J. (2012). *Kehittämistutkimus opinnäytetyönä*. Jyväskylän ammattikorkeakoulu.

Kokkonen T. (2016). Architecture for the Cyber Security Situational Awareness System. In O. Galinina, S. Balandin, Y. Koucheryavy (eds.) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2016, ruSMART 2016. Lecture Notes in Computer Science, vol. 9870, 294-302.

Kokkonen, T., Hautamäki, J., Siltanen, J. & Hämäläinen, T. (2016). *Model for Sharing the Information of Cyber Security Situation Awareness between Organizations.* 23rd International Conference on Telecommunications (ICT)

Kookjin, K., Jaepil, Y., Sukjoon, Y., Jiwon, K., Kyungshin, K. & Dongkyoo, S. (2023*). Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness.* Applied Sciences. 2023; 13(4):2331.

Lehto M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). *Strategic management of cyber security in Finland.* Prime Minister´s Office. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y

McGuinness B. and Foy L., (2000). *A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS)*. First Human Performance, Situation Awareness and Automation Conference, Savannah, Georgia, 2000.

Mustajärvi, R. (2023). *Impact of SOC Pilot Implementation on Situational Picture: Analysis and Application to Security Management.* Centria University of Applied Sciences

National Emergency Supply Agency. (2022). Toimialojen kyberkypsyyden selvitys 2022. Retrieved from https://www.digipooli.fi/sites/digipooli/files/inline-files/HVK_Toimialojen%20kyberkypsyyden%20selvitys%202022.pdf

Onwubiko, C. (2016). *Understanding Cyber Situation Awareness*. International Journal on Cyber Situational Awareness, Vol. 1, No. 1, pp. 11—30.

Ortamo, S. (2024). *Venäjä näyttää nyt tekevän kyberiskuja länsimaiden vesilaitoksiin – Mikko Hyppönen: ”Aikamoinen uutinen”*. Yle news. Retrieved from https://yle.fi/a/74-20084689

Ozkaya, E. (2022). *Practical Cyber Threat Intelligence: Gather, Process, and Analyze Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices*. BPB Online LLP.

Pahlevan, M., Voulkidis, A., & Velivassaki, T.-H. (2021). *Secure exchange of cyber threat intelligence using TAXII and distributed ledger technologies - Application for electrical power and energy system.* In Proceedings of International Conference on Availability, Reliability and Security, ARES 2021 Article 122 ACM.

Pöyhönen, J., Nuojua,V., Lehto, M. & Rajamäki, J. (2019). *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations.* Information & Security: An International Journal 43:2, 236-256.

Pöyhönen, J., Rajamäki, J., Nuojua, V., & Lehto, M. (2021). *Cyber Situational Awareness in Critical Infrastructure Organizations.* In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies (pp. 161-178).

Rizov, V. (2016). *Information sharing for cyber threats*. Information & Security: An International Journal. v.39:1, 2018, 43-50.

Salomaa, J. (2019), *Measuring and Creating Situational Awareness in Cybersecurity: The Requirements Specification for Situational Awareness and Metrics Platform*. South-Eastern Finland university of applied sciences.

Security Committee, (2017). *Vocabulary of Comprehensive Security*. Sanastokeskus. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Security Committee, 2018. *Vocabulary of Cyber Security*. Sanastokeskus. Retrieved from https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Skopik, F., Bonitz, A., Grantz, V., & Göhler, G. (2022). *From scattered data to actionable knowledge: Flexible cyber security reporting in the military domain*. International Journal of Information Security, 21(6), 1323-1347.

Teriö, J. (2017). *Toward cyber situational awareness with open source software*. University of Jyväskylä.

The Finnish Security Intelligence Service, (2024). *Suojelupoliisin vuosikirja 2023*. Retrieved from https://vuosikirja.supo.fi/documents/62399122/66519032/SUPO+Yearbook+2023.pdf/d315b9ee-0039-c99b-5f2d-fbc3672f6be7/SUPO+Yearbook+2023.pdf?t=1711366635064

The Ministry of Finance. (2020). *Digital Security in the Public Sector*. Publications of the Ministry of Finance – 2020:45. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162265/VM_2020_45.pdf?sequence=1&isAllowed=y

The Ministry of Finance. (2022*). Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys*. Publications of the Ministry of Finance – 2022:76. Retrieved from https://api.hankeikkuna.fi/asiakirjat/a1a3d28d-4014-454a-b9ae-6e3cb655dc55/90b5a468-9a83-4789-b195-bbfc087c0ebc/JULKAISU_20240221131007.pdf

The Ministry of Finance. *Structures, guidance and direction of administration.* Retrieved from https://vm.fi/hallintopolitiikka/hallinnon-rakenteet

The Ministry of Justice. (2023*). Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi*. Lausuntopalvelu. Retrieved from https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd

The MITRE Corporation. (2012). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* Retrieved from https://www.mitre.org/sites/default/files/publications/stix.pdf

The MITRE Corporation. (2013). *Structured Threat Information eXpression — STIX™ A Structured Language for Cyber Threat Intelligence Information.*

The National Cyber Security Center (2023). *Tietoturvan vuosi 2022*. Retrieved from https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Tietoturvan-vuosi-2022.pdf

The Security Committee. (2017). *The Security Strategy for Society*. The Security Committee.

Tianfield, H. (2017). *Cyber security situational awareness*. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, p. 782-787.

Yasseri, S. (2012). *Marine Domain Awareness and Safety of Heavy Lift Operation.* Marine Heavy Transport & Lift III, 24–25 October 2012, London, UK