

MASTER THESIS

Security Operations (SecOps) and the Internet of Things (IoT)

Introducing IoT security monitoring

Per-Arne Jørgensen
9th June 2023

Master in Applied Computer Science
Faculty of Computer Science, Engineering and Economics



Abstract

Security Operation Centres (SOC) has been operating in the IT domain for several years, focusing on developing skills and experience pertaining to businesses' impacts of cyber security incidents, e.g., with regard to downtime and recovery processes. Now, the introduction of IoT devices in both mission-critical systems, as well as enterprise IT systems and services, creates an even more complex system landscape. Preparing and training cyber security for this landscape is challenging as existing practices might not be sufficient.

A SOC faces different challenges in the establishment of a unified security monitoring process for IoT devices. The implied factors of closed ecosystems, vendor lock-ins and complex IoT management deployments make this a challenge. IoT-related attacks have become more visible in recent years and comprise a challenge with complexity in handling and mitigating an increasing number of IoT devices. The deployment of unmanaged IoT devices without proper security monitoring can introduce a risk for businesses that potentially can impact both physical processes and the logical level of IoT devices originating from the cyber domain. Finding a suitable response plan to such incidents can be challenging to mitigate in time.

How can a SOC develop an effective response plan for IoT attacks? Well, that depends on several elements, but by means, of knowing the existence of IoT devices and their purpose in line with the business. There is a need to detect and identify different types of attacks before an impact strikes and as early in the detection phase find an effective response plan to use. What is the state of the art and practices today? We know that time to respond is often crucial to limit the damage and reduce the impact of a successful cyber-attack. Different types of incidents require different response strategies for mitigation. How prepared are the Security Operation Centres to level up with the increasing number of IoT systems being deployed and the demands from the business?

The presented work is performed as qualitative research addressing the state of practice in SOC teams with regard to the introduction of IoT and relevant challenges and solutions. Six interviews have been performed with security professionals from different private- and public organisations in Norway. The interviews have been organised using thematic analysis and analysed from the perspective of a SOC. Results are discussed with regard to different themes to identify challenges and best practices to support the introduction of IoT devices in SOC operations.

With this qualitative research, we hope to bring more knowledge about the different security operation centres' perspectives on the security monitoring of IoT devices and ecosystems.

Acknowledgments

I thank my supervisor at Østfold University College, professor Øystein Haugen, for his dedicated collaboration, support and constructive feedback during this master project and program.

I also want to thank my employer, Institute for Energy Technology and Dr. Bjørn Axel Gran, for believing in me and making it possible to combine work with studying. The support from colleagues has been highly appreciated and I'm grateful for their encouragement, feedback and proofreading.

Lastly, a big hug and thanks to my supporting family Nicolai, Aurora and Ulrik, and a special one to my lovely wife, Cathrine for her patience. This wouldn't be possible without her support and effort at home.

About me and this thesis

This master's thesis is written during Autumn 2022 and Spring 2023, for the cyber-physical systems program in applied computer science at Østfold University College in Halden. I have taken this master's program part-time and combined it with full-time work at Institute for Energy Technology as head of security operations.

Per-Arne Jørgensen
Halden, 9th June 2023

Prerequisites

The reader should know that I have used the "we" formulation instead of "I" to tell the story during this master thesis to engage together with the reader.

Contents

Abstract	3
Acknowledgments	5
About me and this thesis	7
Prerequisites	9
Contents	11
List of Figures	13
List of Tables	15
Acronyms	17
1 Introduction	1
1.1 Motivation	1
1.2 Problem statement	2
1.3 Research objectives	4
1.4 Research questions	4
1.5 Structure of the master thesis	5
2 State of the art	7
2.1 Researching the topic	7
2.2 A state of the art overview of SOC and IoT	11
3 Methodology	21
3.1 Research design and methodology	21
3.2 The semi-structured interviews approach	22
3.3 Planning the interview process	24
3.4 Qualitative data collection	25
3.5 Analysis methodology	25
4 Results and analysis	35
4.1 Analysis of interviews	37
4.2 Business drivers	38
4.3 IoT management	43
4.4 Monitoring and detection	49

4.5	Security Operation Centre (SOC)	55
4.6	A quantitative summary of the result	62
5	Discussion	65
5.1	RQ1: What are the challenges in security monitoring, maintaining and operating IoT devices?	65
5.2	RQ2: What type of data is collected from IoT devices to detect anomalies and what information does this relay on?	71
5.3	RQ3: How should SOCs operate and work in the future to adapt to monitor the increasing number of IoT devices?	77
5.4	Threats to validity	82
6	Conclusion and future work	83
6.1	Conclusion	83
6.2	Future work	84
	Bibliography	85
A	Interview guide	91
B	Interview and consent formular	113
C	Qualitative Data Analysis	117
D	COREQ checklist	119
E	Theme maps	123
F	A summary of state of the art aspects of SOC and IoT	131
G	Thematic Analysis	135

List of Figures

1.1	DevSecOps Model - Source: https://miro.medium.com/max/1082/0*8zmHcgGpZnH26fcX	3
2.1	The snowballing process (Wohlin, 2014)	8
3.1	The methodology	22
3.2	The IoT domain and research perspectives	23
4.1	The interview process in time	35
4.2	The mapping of SOCs system focus in relation to the VENN-diagram	38
4.3	Business drivers mapping of themes for IQ1	40
4.4	Business drivers mapping of themes for IQ2	42
4.5	Business drivers mapping of themes for IQ3	43
4.6	IoT Management mapping of themes for IQ4	45
4.7	IoT Management mapping of themes for IQ5	47
4.8	IoT Management mapping of themes for IQ6	49
4.9	Monitoring and detection of themes for IQ7	53
4.10	Monitoring and detection mapping of themes for IQ8	54
4.11	Monitoring and detection mapping of themes for IQ9	55
4.12	Security Operation Centre mapping of themes for IQ10	58
4.13	Security Operation Centre mapping of themes for IQ11	59
4.14	Security Operation Centre mapping of themes for IQ12	61
4.15	Security Operation Centre mapping of themes for IQ13	62
4.16	Total number of answers (statements) from each SOC	64
4.17	Number of answers (statements) from each SOC distributed by IQ	64
5.1	The map of SOC challenges for IQ3, IQ5, IQ7 and IQ12 addressing logging, monitoring, detection and operation within the IoT-, OT- and IIoT domain.	66
5.2	A map of metrics, events and alarms statements for IQ4, IQ6, IQ7, IQ8 and IQ9 addressing IoT management, monitoring and detection from the IoT domain.	72
5.3	A map of threats and vulnerabilities statements for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13 addressing business drivers, monitoring and detection, and SOC from the IoT domain.	77
5.4	A map of human and organisational factor statements for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13 addressing business drivers, monitoring and detection, and SOC from the IoT domain.	79

List of Tables

2.1	Search strings	8
2.2	First search string iteration	9
2.3	Second search string iteration	10
2.4	Third search string iteration	10
2.5	Fourth search string iteration	11
2.6	IoT challenges summarised	13
2.7	Threats summarised	15
2.8	Vulnerabilities summarised	15
3.1	Topic mapping schema with initial coding and answering the RQs through IQs.	26
3.2	Validity scoring system	28
3.3	Refined themes	33
3.4	Topic mapping schema with the refined themes .	34
4.1	Interview candidates affiliation	36
4.2	Analysis of "business drivers" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.	39
4.3	Analysis of "IoT management" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.	44
4.4	Analysis of "monitoring and detection" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.	50
4.5	Analysis of "SOC" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.	56
4.6	A quantitative overview of the result using thematic analysis to present identified themes with statements to answer IQs.	63
5.1	Data collected and analysed from the theme "metrics, events and alarms" with indicators relevant for anomaly detection.	74

Acronyms

- BMS** Building Management System. [1](#)
- CERT** Computer Emergency Response Team. [22](#)
- CPU** Central Processing Unit. [20](#), [75](#), [76](#)
- CVSS** Common Vulnerability Scoring System. [51](#)
- DCS** Distributed Control Systems. [45](#)
- DDOS** Distributed Denial of Service. [17](#)
- EDR** Endpoint Detection and Response. [48](#)
- HVAC** Heating, Ventilation, and Air Conditioning. [1](#)
- ICS** Industrial Control System. [14](#), [16](#), [44](#), [67](#), [70](#), [72](#)
- IDS** Intrusion Detection System. [16–18](#)
- IIoT** Industrial internet of things. [14](#), [16](#), [17](#), [37](#), [38](#), [45](#), [70](#), [77](#), [79](#)
- IoT** Internet of things. [2–5](#), [7](#), [11–23](#), [29–32](#), [37–54](#), [56–58](#), [60–62](#), [65](#), [66](#), [68](#), [70](#), [71](#), [75–84](#)
- IRT** Incident Response Team. [22](#)
- IT** Informational technology. [2](#), [4](#), [13](#), [16](#), [18](#), [19](#), [23](#), [35](#), [38](#), [39](#), [41](#), [45](#), [51](#), [62](#), [65](#), [67–69](#), [71](#), [79–81](#), [83](#)
- KPI** Key Performance Indicators. [80](#)
- MEC** Multi-access Edge Computing. [16](#)
- ML** Machine Learning. [16](#)
- MQTT** Message Ques Telemetry Transport. [19](#)
- OT** Operational Technology. [2](#), [13](#), [16](#), [18–20](#), [23](#), [35](#), [37–41](#), [43–45](#), [51](#), [57](#), [59](#), [62](#), [65](#), [67–71](#), [75](#), [77](#), [79](#), [80](#), [83](#), [84](#)
- PLC** Programmable logic controller. [38](#), [47](#), [51](#), [75](#)

QoS Quality of Service. [17](#)

SIEM Security Information and Event Management system. [14](#), [54](#), [72](#), [76](#)

SOC Security operations centre. [1](#), [4](#), [5](#), [7](#), [11](#), [13–16](#), [18](#), [20–22](#), [24](#), [30–32](#), [37–40](#), [48](#), [49](#), [51](#), [53](#), [55–63](#), [65](#), [67–72](#), [75](#), [77–81](#), [83](#), [84](#)

SQL Structured Query Language. [17](#)

USB Universal Serial Bus. [75](#)

Chapter 1

Introduction

1.1 Motivation

In this master thesis, we investigate how the Security Operation Centres (SOC) would approach and practice security monitoring of IoT devices in an emerging system landscape within different businesses. The motivation for this was based on the researcher's own experience during establishing a SOC within a mission-critical business. During the establishment of the SOC and the first year of operations, we experienced inconstancy in how to deal with IoT devices, herein a lack of best-practice in the industry in general on how to introduce such systems for logging and security monitoring.

The current view of the empirical scientific peer-reviewed journals, papers and sources should be further explored to find clear answers on how to introduce IoT devices for security monitoring in a SOC setting. The diversity of different types of IoT devices for different purposes presented by other organisational units seems to go "under the radar" of the SOC and could potentially introduce a risk for the business. With the urgent need to address aspects of security introduced for operating, maintaining and monitoring IoT devices by a SOC, we explore the current situation regarding IoT devices and how these perspectives were interpreted by a SOC for security monitoring.

The building management system (BMS) is one example where IoT has been a valuable add-on providing wireless capabilities to reduce the cost of wiring buildings with sensors and actuators. A BMS consists of hardware, software and networking to streamline the operation of a building's electrical and mechanical equipment (Wallin, 2022). The buildings were instrumented with smartness in mind for energy optimisation and control of HVAC¹ systems. However, the stakeholders of such systems were often different organisational units or outsourced to others regulated by rental agreements without ownership of the system. Nevertheless, as BMS often is the heart of monitoring and controlling a building it must be protected accordingly from both external physical- and cyber threats. How are these systems acquired? Which functional and non-functional requirements were used? Which network protocols are used? How is the system connected? Is it available on the Internet? How are these systems maintained and updated? Is security monitoring considered for these systems? There are several questions that need answers for a holistic overview of the current system landscape.

Another example is the use of industrial IoT devices in conditional monitoring of pumps or actuators for predictive maintenance with the purpose of monitoring the equipment for an extended lifetime. Existing infrastructures were often equipped with cheaper add-on IoT sensors

¹Heating, Ventilation, and Air Conditioning (HVAC)

for health monitoring and connected to the corporate network. However, the same questions above apply. The suppliers play a central role in such ecosystems. The supply chain is something that has been addressed with business risks in recent years. According to the European Union Agency for Cybersecurity (ENISA), the supply chain is defined as "a system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer" (ENISA, 2015). Business stakeholders rely on the suppliers to maintain security and control the IoT solution. But how well are these established agreements followed up in practice by the customer? Unsecured and unmanaged IoT devices can potentially become an attack vector for threat actors. One example is the Supply chain attack on SolarWinds² where a threat actor injected malicious software into the Orion³ product during the build process which has been used to gain access to suppliers and end-users network infrastructure (ENISA, 2021, p. 15). Another example was an attack on a BMS that utilised a weakness in a security feature of the KNX⁴ protocol to lock out the client from the system and deleted the configuration (Jackson Higgins, 2021).

1.2 Problem statement

Modern society relies heavily on the use of innovative solutions driven by the Internet of Things (IoT) to build the future for human health and economic growth. An IoT device is a "thing" that connects to the internet and can be defined as a "network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information" (C. C. NIST, 2022). The Internet of Things paradigm shifts towards a growing trend of low-cost IoT devices connecting to the Internet to make "things" smarter by collecting and analysing data from a variety of sensors and actuators. IoT devices are present in many domains throughout our society, i.e., from manufacturing industries and smart cities to agriculture. Low-cost devices emerge into our daily lives from use in private households to businesses and industries. Solving different use cases from monitoring and controlling business-critical manufacturing lines to a simple temperature monitoring device in a resident controlling a heater.

However, the number of connected devices is growing and has exceeded 12.3 billion devices globally (Analytics, 2021) as of 2021. The complexity introduced by operating such an ecosystem of IoT systems related to security and safety also introduces vulnerabilities and threats into existing information technology- (IT) and operational technology (OT) infrastructures. Security is still a high-priority challenge to maintain the confidentiality, integrity, and availability (CIA) in IoT devices (Khan et al., 2020) and data processing and management. Addressing issues like privacy, lack of encryption, insufficient testing and updating, the risk of not changing default passwords and IoT malware is existing and persistent. Monitoring and maintaining an up-to-date IoT fleet is cumbersome without efficient tools or systems when building resiliency into IoT platforms. This is key essential information for a security operation centre (SOC) when working on preventing successful cyber-attacks for businesses and governments. This is a challenging task that requires more standardization and security solutions built into such IoT systems to achieve better insight and knowledge on threats and mitigating vulnerabilities.

An IoT device consists of different components and can be described with some basic levels divided into at least three layers comprised of the physical hardware, an operating system and communication capabilities (Weissman & Jayasumana, 2020). The type of IoT device can be (1)

²<https://www.solarwinds.com/>

³<https://www.solarwinds.com/solutions/orion>

⁴<https://radiocrafts.com/technologies/knx-technology-overview/>

a microcontroller or embedded system combined with a Central Processing Unit (CPU), memory (RAM) and storage on a single chip, or a (2) System-On-Chip (SoC). The IoT device provides different interfaces for connecting sensors with connectivity capabilities and has limited data processing. Insight into how an IoT behaves and performs may require a different approach in the future and should rely on a secure development lifecycle (SDL) process with extensive libraries and code practice to enable better monitoring capabilities and logging features for detecting anomalies, over the air upgrades and management tools for control to mention some.

The agile development processes have become the new de facto standard for the most modern software developing methods when building new products these days. This introduces new possibilities in the design phase enabling the alignment of different disciplines when addressing more rapid development and the operations of new products or services. This type of operating model in software development has been introduced when merging development and operations perspectives and has become the movement called DevOps. According to Amazon “DevOps is the combination of cultural philosophies, practices, and tools that increases an organization’s ability to deliver applications and services at high velocity” (AWS, 2022). Higher demands in availability utilised by cloud-connected applications and devices with the ability to scale on demand has become a requirement from the businesses, but also continuity which includes reliability and security. However, the DevOps model has been positively adopted by enterprises and can by means also be extended to address the lack of security. Security is often left out and is applied later. Incorporating security into the design process with a DevSecOps perspective can bring “IT development, IT operations, and security principles closer together, to make technology products more robust.” (Callum, 2022). This beneficiary brings new requirements and the need for continuous monitoring and insights into applications, services, and devices. “When utilizing continuous integration/continuous deployment (CI/CD) practices paired with monitoring tools, you will be able to gain better visibility into your application health and proactively identify and mitigate risks to reduce exposure to attacks.” (Security, 2022). However, a layer of complexity requires new tools and services that potentially build an ecosystem of systems. Figure 1.1 shows an overview of a DevSecOps model with phases and processes for continuous integration and delivery integrated with security operation, patching, logging, and penetration testing. The model enables continuous monitoring capabilities in IoT networks for Security Operation Centers.



Figure 1.1: DevSecOps Model - Source: https://miro.medium.com/max/1082/0*8zmHcgGpZnH26fcX

According to Peiris et al. (2021), the definition of a Security Operation Center (SOC) is a “centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents” (Peiris et al., 2021). In recent years the emerging need of having dedicated and skilled people working with operational security and handling incidents to solve business issues is seen as a pre-requisite for companies in the 21st century. In parallel with even more serious and prevalent cyber-attacks, the number of attacks is rising exponentially in the IoT domain. There is a need of collecting telemetry data and logs from IoT devices across the enterprise to gain insights and visibility about the assets that are vital information for a SOC to analyse. These solutions are becoming a System of System (SOS) and the "Guide to the Systems Engineering Body of Knowledge (SEBoK)" defines it as a "Set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own." (Henshaw et al., 2022)

1.3 Research objectives

The goal of this research is to bring more knowledge about IoT devices in the current system landscape within established SOC's by:

- Identify the SOC's challenges in security monitoring and maintaining IoT devices and systems over time.
- Identify SOC's awareness about IoT systems and devices' existence for security monitoring
- Identify which monitoring techniques and parameters that would be effective measures for IoT security monitoring.
- Identify how SOC's should onboard IoT systems and devices for optimal detection.

1.4 Research questions

The following research questions are raised to bring more knowledge about the IoT domain on how a SOC can integrate or incorporate insights from heterogeneous IoT networks comprised of a sensor, connected to hardware running a piece of software processing and generating data to be transferred using wired or wireless connectivity for further analysis and usage. With an IoT fleet of thousands of sensors and actuators, general IT monitoring tools and methods may be insufficient. By reviewing the literature, we seek to find how security operation centres (SOC) can adapt to be able to monitor IoT devices in future distributed architectures involving a system from the systems perspective.

RQ1: What are the challenges in security monitoring, maintaining and operating IoT devices?

[RQ1.1:] What is the challenge seen from the SOC's perspective on monitoring IoT devices?

[RQ1.2:] What is the state-of-practice for monitoring IoT devices?

RQ2: What type of data is collected from IoT devices to detect anomalies and what information does this rely on?

[RQ2.1:] What type of remediation methods are used to mitigate IoT security alarms and incidents?

RQ3: How should a SOC operate and work in the future to adapt to monitor the increasing number of IoT devices?

[RQ3.1:] What does this depend on?

1.5 Structure of the master thesis

This master thesis is structured in the following sections:

- Chapter 2 - Investigate state of the art
- Chapter 3 - Specifying methodology
 - Chapter 3.1 - The plan
 - Chapter 3.2 - Identifying and developing 13 interview questions
 - Chapter 3.3 - Data collection
 - Chapter 3.4 - Analysing data
- Chapter 4 - Collecting and analysing data from interviewing SOCs
- Chapter 5 - Discussion
- Chapter 6 - Conclusion and future work

Chapter 2

State of the art

2.1 Researching the topic

We will research the problem using existing empirical scientific sources and conduct a literature review on [SOC](#) and [IoT](#) with regard to threats and vulnerabilities, and security monitoring from detection to the handling of security incidents.

2.1.1 Literature review using the Snowballing process

The literature review is conducted using the snowballing method introduced by Wohlin (2014) to identify and find relevant literature on the topic. The first (1) stage is to do a literature search to identify relevant articles and journal papers for a basis to start with. We choose Google Scholar for searching the literature as this provides searches in multiple academic sources. Finding relevant papers on the topic required a broader search area to cover different aspects of a security operations centre's (SOC) perspective on how to get insights on [IoT](#) device monitoring by combining different search strings. The second (2) stage is to select a start-set of relevant articles and papers, followed by the snowballing process (3) stage to find similar papers of interest referenced, but also exclude papers that don't meet the basic criteria. The last stage (4) in the process is the result of selected papers for the final literature review.

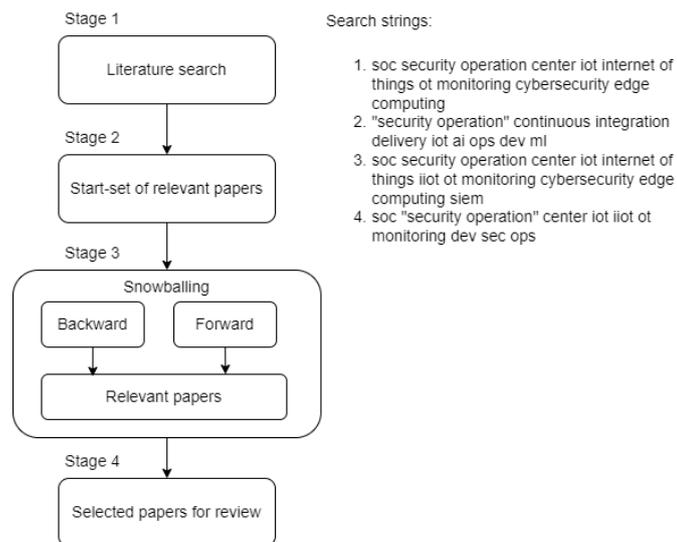


Figure 2.1: The snowballing process (Wohlin, 2014)

2.1.2 Literature search

The search strings for the start-set of papers were selected by the generic criteria as (1) the title of the paper, (2) the time frame from 2018 for the most up-to-date articles and (3) the number of citations. Identifying papers for the start-set was based on four (4) search string sets as shown in the table below.

Table 2.1: Search strings

Iteration	Search strings and syntax	Filter	Number of articles found	Selected start-set
1	soc security operation center iot internet of things iiot ot monitoring cybersecurity edge computing	After 2018	5310	7
2	"security operation" continuous integration delivery iot ai ops dev ml	After 2018	80	4
3	soc security operation center iot internet of things iiot ot monitoring cybersecurity edge computing siem	After 2018	165	5
4	soc "security operation" center iot iiot ot monitoring dev sec ops	After 2018	71	8
Start-set				24

The start-set of the selected article must contain the word “security operation” or “IoT” as a minimum. Selecting only sources that were open and available from the Østfold University College library subscriptions, and online materials (i.e. books) that required additional payment options were not selected.

From the first search iteration with the search string “soc security operation center iot internet of things iiot ot monitoring cybersecurity edge computing” the result provided was 5310 hits. From this search result only the five (5) first pages from Google Scholar were visited and the seven (7) selected articles were chosen by the number of citations and its title as presented in the table 2.2.

Table 2.2: First search string iteration

Iteration	Title	Reference	Citations	Pub. year
1	Security Operations Center: A Systematic Study and Open Challenges.	(Vielberth et al., 2020)	19	2020
1	Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives.	(Ni et al., 2019)	58	2019
1	Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges.	(T. Qiu et al., 2020)	106	2020
1	A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things.	(Alwarafy et al., 2021)	48	2021
1	Survey on Multi-Access Edge Computing for Internet of Things Realization.	(Porambage et al., 2018)	410	2018
1	Edge computing for Internet of Things: A survey, e-healthcare case study and future direction.	(Ray et al., 2019)	86	2019
1	Industrial internet of things: Recent advances, enabling technologies and open challenges.	(Khan et al., 2020)	190	2020

In the second iteration, the search string was modified and extended to cover topics influenced by AIOps, DevOps and machine learning: (“security operation” continuous integration delivery iot ai ops dev ml”). The result was 80 articles that were screened and selected by the defined criteria. A recent article from within the current year 2022 was also selected despite the zero citations marking but included by its relevance from the title.

Table 2.3: Second search string iteration

Iteration	Title	Reference	Citations	Pub. year
2	An architecture to manage security operations for digital service chains.	(Repetto et al., 2021)	7	2021
2	An Agile AI and IoT-Augmented Smart Farming: A Cost-Effective Cognitive Weather Station.	(Faid et al., 2022)	0	2022
2	Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats	(Furdek et al., 2020)	10	2021
2	Industrial control systems integrations to Operation Technology and Information Technology Security Operation Center.	(Rajamäki, 2021)	0	2021

Based on the previous search results the security information and event management (SIEM) were mentioned several times and for the third search string operation the string “siem” were added. The following selected article from the third iteration was added to the start-set.

Table 2.4: Third search string iteration

Iteration	Title	Reference	Citations	Pub. year
3	Network Intrusion Detection for IoT Security Based on Learning Techniques.	(Chaabouni et al., 2019)	312	2019
3	Internet of Things (IoT) and the Energy Sector.	(Hossein Motlagh et al., 2020)	171	2020
3	A security monitoring system for internet of things.	(Casola, De Benedictis, Riccio et al., 2019)	23	2019
3	Anatomy of Threats to the Internet of Things.	(Makhdoom et al., 2019)	172	2019
3	Fog Computing Enabling Industrial Internet of Things: State-of-the-Art and Research Challenges.	(Basir et al., 2019)	56	2019

The last search operation was modified and extended with “dev sec ops” to reflect topics relevant to IoT device management for continuous monitoring and upgrading by combining the software development (dev) and IT operations (ops).

Table 2.5: Fourth search string iteration

Iteration	Title	Reference	Citations	Pub. year
4	Big Data Analytics on Cyber Attack Graphs for Prioritizing Agile Security Requirements.	(Hadar & Hassanzadeh, 2019)	12	2019
4	Review of Industry 4.0 Security Challenges.	(Ferencz et al., 2021)	1	2021
4	Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies.	(Hamad et al., 2020)	40	2020
4	Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions.	(Urooj et al., 2022)	2	2022
4	Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems.	(Tagarev & Sharkov, 2019)	3	2019
4	Securing connection between IT and OT: The Fog Intrusion Detection System prospective.	(Colelli et al., 2019)	134	2019
4	Security Standards and Measures for Massive IoT in the 5G Era.	(Q. Qiu et al., 2021)	0	2021
4	Grasp on next generation security operation centre NGSOC): Comparative study.	(Dun et al., 2021)	1	2021

Using backwards and forward (Wohlin, [2014](#)) snowballing method on the defined start-set to identify new papers to be included by citation reference list was done, but also excluding papers that did not fulfil the basic criteria like publication date and non-peer reviewed papers. With forward snowballing the abstract, language and title were evaluated, and papers were included in the start-set.

To summarise; the snowballing method that was taken from the first selected start-set of 24 papers; 10 new relevant papers were found from the four search operations and were selected for inclusion from the backwards reference list. Additional 4 papers from the first start-set were excluded based on abstract and title. A total of 30 papers were selected and made the selected start-set of papers for review. In Appendix F we provide an overview of the sorting and organising of the literature based on the different aspects of [SOC](#) and [IoT](#) domain. The aspect is based on identified topics during the read-through of the papers to help categorise and sort. The different aspect was categorised as monitoring, [SOC](#) operating models, communication technologies, cyber threats and vulnerabilities, cyber governance processes etc.

2.2 A state of the art overview of SOC and IoT

Reviewing the most recent development within the [IoT](#) domain literature, with the perspective on how a SOC could monitor, maintain and operate [IoT](#) devices, will be further discussed. However,

the literature from 2018 to 2022 is still arguing and addressing security challenges with problems related to heterogeneous IoT devices and networks, vulnerabilities and monitoring issues related to limited resources. According to Hewlett Packard (HP) security monitoring “involves collecting and analysing information to detect suspicious behaviour or unauthorised system changes on your network, defining which types of behaviour should trigger alerts, and taking action on alerts as needed.” (Hewlett Packard, 2022). Another definition of security monitoring is from NIST, where the risk and organizational perspectives are addressed. The responsibility for operating a SOC would be to “Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.” (NIST, 2022).

2.2.1 IoT challenges

The IoT challenges are severe and Hossein Motlagh et al. (2020) presented an overview of issues viable for the energy sector of applying IoT. The authors have summarised the challenges and is addressing the architecture design to provide reliable end-to-end connection, the integration of IoT and data management and poor adoption of standardisation with inconsistency in IoT devices and capabilities to mention some Hossein Motlagh et al. (2020). A paper from (Khan et al., 2020) is a review of recent advances in enabling technologies on industry IoT and addresses security and privacy as one of the major open challenges. In addition, there is an interesting statement about IoT and the open challenges in the management of IoT devices; “the configuration, deployment, monitoring, and maintenance of these devices is a challenging task and require highly qualified technical staff” (Khan et al., 2020). The IoT security challenges permeate hardware, connectivity, and data layers. In the table below, some of these challenges were summarised.

Table 2.6: IoT challenges summarised

Layer	Challenge	Reference	
Hardware	Protect against risks from security vulnerabilities. Long lifecycle of systems, legacy equipment	(Khan et al., 2020)	
	Protect against risks from security vulnerabilities. Long lifecycle of systems, legacy equipment	(Khan et al., 2020)	
	Limited resources (CPU, memory)	(Faid et al., 2022)	
	Low power, low computing power, small disk space	(Makhdoom et al., 2019) (Khan et al., 2020)	
	Lack of IoT standardization	(Khan et al., 2020)	
	Resource exhaustion	(Rapuzzi & Repetto, 2018)	
	Tampering; access to console, I/O ports	(Rapuzzi & Repetto, 2018)	
	Heterogeneous IoT hardware devices	(Hadar & Hassanzadeh, 2019)	
	Poor configuration: weak security mechanism by design i.e., access control	(Rapuzzi & Repetto, 2018)	
	Timestamp inconsistency	(Rajamäki, 2021)	
	Poor adoption of standards	(Hossein Motlagh et al., 2020)	
	Connectivity	Communication delays, latency	(Khan et al., 2020)
		Light communication protocols	(Faid et al., 2022)
Secure remote access		(Ferencz et al., 2021)	
Neglected security testing		(Dimitrov & Syarova, 2019)	
No authentication and encryption		(Makhdoom et al., 2019)	
Heterogeneous IoT network protocols		(Hadar & Hassanzadeh, 2019)	
IoT devices directly connected to the Internet		(Casola, De Benedictis, Riccio et al., 2019)	
Data	No security and privacy in protecting information (data management)	(Hossein Motlagh et al., 2020) (Makhdoom et al., 2019)	
	Poor or no encryption capabilities of data stored on IoT device	(Basir et al., 2019)	
	Data leakage	(Ferencz et al., 2021)	

2.2.2 Different SOC operating models

Back in 2010, security was often something the internal IT people had to manage in addition to IT operations. In recent years this task has been dedicated to a Security Operations Centre (SOC) which is an operational function inside an enterprise company given the mandate to detect and respond to cyber threats. The responsibility of handling security incidents and response for mitigation is given to security operation centres. Operating a SOC is a complex task. Nowadays, there is an emerging need to extend the SOC function to also monitor IoT and OT, not only enterprise IT.

In a recent study from Vielberth et al. (2020) they describe the importance of each building block and component when setting up a SOC. The authors are addressing the challenges when it comes

to the integration of people, processes and technology with governance and compliance aspects. The balance between those aspects is important for how to operate and maintain detection and monitoring capabilities. However, IoT monitoring seen from a SOC's perspective is more technology driven. The aim of the study done by Dun et al. (2021) was to make a foundation on how to develop "a modern system of systematic operation centres for the next generation (NGSOC) for IIoT climate" (Dun et al., 2021). The next generation SOC is introduced by Dun et al. (2021) and consists of a balance between the building blocks made of people (skills and knowledge), process (organisational factors and interfaces) and technology (insights and tools) to pace with the emerging threats and vulnerabilities. Nevertheless, the main goal for a SOC is to prevent successful cyber-attacks and focus on proactive operations including monitoring and detection. With the vast amount of information gathered through monitoring of system indicators, there must be available capabilities to analyse this information with context from the SOC's with human knowledge. This leads to the "need for automation and convergence in cyber-attack prevention, detection and response" (Dun et al., 2021, p.872).

Repetto et al. (2021) have argued and suggested an architecture for an operational SOC model to differentiate between the control and management interface from the data interface to develop a SOC as a service using microservices and data mesh technologies. The authors are trying to close the current gap with the lack of insight available from IoT devices and suggest distributed infrastructure services, aka system-of-system approach, with built-in features for a distributed event and log processing, performance monitoring, detection of anomalies and secure management. Existing enterprise paradigms on security rely on legacy methods and models for protecting the perimeters with a defence-in-depth strategy and security appliances (i.e., firewalls, application firewalls, intrusion detection systems, etc.) placed on the borderline between the enterprise and the internet. Each of these appliances is handling different security aspects as silos and it's hard to overcome the overhead of management and monitoring for a holistic overview of the threats and vulnerabilities in the cyber domain. Therefore, there is an increasing need for a new generation of cyber-security paradigms that can permeate into more distributed and multi-domain systems. According to Rapuzzi and Repetto (2018) the "complexity and multi-vector nature of recent cyber-security threats require a transition from current narrow-scope silos to a more integrated multi-vendor layered and open framework" (Rapuzzi & Repetto, 2018, p.31).

Goodall et al. (2018) made a prototype of an application for anomaly detection tested in a SOC setting to give SOC Analysts input on the detection and classification of attacks in networks for situation awareness. The study does not mention IoT devices, but for heterogeneous networks, this could be linked to network parameters to distinguish between different IoT traffic.

Dimitrov and Syarova (2019) describes the different perspectives of integrating the shared ICS Security Operation Centre concept to deliver competence and functionalities for different stakeholders to help protect against cyber-attacks. In general ICS systems lack the interoperability for integrating effective security protection. The author suggests, based on experience, that a shared SOC is a comprehensive solution for first-level security operations in such a way that asset owners can focus on OT operations. Similar incidents can be managed and solved faster from multiple ICS systems. Also, with more logs and data available from each ICS subscriber, the creation of better indicators of compromise can be made for early detection.

Weissman and Jayasumana (2020) introduces an effective SOC solution that is scalable to address IoT monitoring by integrating devices into existing SIEM tools. But with different approaches and perspectives on SOC's people and processes, they describe three types of operating models to distinguish between an internal SOC IoT monitoring team, internal SOC integrated IoT and network infrastructure team, and an outsource IoT monitoring SOC as a managed

service. As in every SOC, the personnel competence and skill set are crucial to understanding how to detect, respond and mitigate attacks. However, within the IoT domain, a deeper knowledge of IoT protocols was required by the SOC personnel and was different from regular enterprise networking relying on existing knowledge within ethernet and Wi-Fi¹ standards.

2.2.3 IoT threats and vulnerabilities

The transformation of society to improve health and life utilised by IoT devices has in recent years been challenged by firmly established systems that have been tested and standardised. With transformation through IoT-enabled devices, we were facing new challenges like fleet management, dispersion in the type of devices, amount of data, sensor type, data resolution, different carriers (communication) and protocols. The current evolvement of attacks and vulnerabilities in the IoT domain has in recent years increased. The main threats to IoT according to Rapuzzi and Repetto (2018) were (1) weak security in web interfaces and network services, (2) poor configuration utilising no encryption or fewer access controls using default credentials and default configuration. Physical tampering (3) of IoT devices accompanied with access to the console or physical ports and removable storage to cause compromised devices.

Table 2.7: Threats summarised

Threats	References
DDOS ² attacks Phishing attacks	(Faid et al., 2022)
Malware	(Repetto et al., 2021)
Man-in-the-middle Physical damage Privacy leakages Privilege escalation Service manipulation	(Roman et al., 2018)

Table 2.8: Vulnerabilities summarised

Vulnerability	References
Password sharing Vulnerable backups	(Faid et al., 2022)
Poor integrity of local security agents Untrusted resources	(Repetto et al., 2021)

2.2.4 IoT and monitoring

According to Hewlett Packard “Given the ubiquitous, unavoidable nature of security risks, quick response time is essential to maintaining system security, and automated, continuous security monitoring is key to quick threat detection and response.” (Hewlet Packard, 2022). Ni et al. (2019) are addressing IoT security challenges in edge IoT devices by describing and suggesting mobile edge computing (MEC) capabilities for offloading computing-intensive operations into fog services

¹Wireless Fidelity

at the edge of the networks. SOC operation is not mentioned. Less on how to monitor IoT devices specifically, more data-oriented. However, the idea of utilising fog computing and services in monitoring IoT devices could be an interesting approach in distributed systems or systems of systems (SOS). IoT and industry IoT (IIoT) are similar in their network architecture according to T. Qiu et al. (2020). Nevertheless, there is a difference in the usage in the different domains, where IoT devices have been adopted by more consumer-oriented use cases for use in residents i.e., monitoring temperature and moisture from the environment. For use in the industry, the IIoT are more oriented toward efficiency and reliability with requirements to integrate existing networks and application protocols. A reference architecture for edge is proposed as one solution to integrate edge computing into IIoT in the future. The proposed solution architecture from the authors does not address security as a feature or component through the architecture model, instead, the edge network security in the IIoT domain mainly focuses on attack detection and defence strategies like how it is from the operation in OT environments.

Porambage et al. (2018) provides an overview of the state-of-the-art technologies required for integration of the multi-access edge computing (MEC) with IoT. The MEC system with radio access networks (RANs) like mobile 5G, Wi-Fi or fixed local network access at the edge of the network. MEC will play a vital role in enabling industry IoT applications in the future by addressing machine-to-machine communication for resiliency, connectivity, and security in the IIoT domain according to Porambage et al. (2018). Further, the development of more complex and high-demand IoT use cases will prevail in a shift into the approach of Tactile Internet where human-to-machine and machine-to-machine interaction is “characterized by ultra low latency with extremely high availability, reliability and security” (Porambage et al., 2018, p.1).

Rajamäki (2021) conducted a master thesis involving a project with the Valmet Automation company on how to integrate ICS systems and log management systems with existing IT-oriented SOC comprised by competence mainly from the IT domain.

Chaabouni et al. (2019) has conducted a survey on network intrusion detection systems (NIDSs) deploying different aspects of machine learning techniques for IoT when malware and botnets attack the IoT domain. The current threat landscape and lack of security measures in the IoT ecosystem are challenging to mitigate with existing signature-based IDS techniques. The fact that “compromising a single component and/or communication channels in IoT-based systems can paralyze the part or complete Internet network” (Chaabouni et al., 2019, p.1) the authors introduce other more efficient techniques using machine learning (ML). ML techniques can be challenged to cope with the amount of IoT devices and true-positive detections mechanism. Especially, when relying on IoT technology for critical functions in our society. Using network IDS with ML detection techniques seems to be an effective measure in particular cases.

Benkhelifa et al. (2018) provides a survey on intrusion detection systems for IoT based on network parameters and heterogeneous IoT device types. For the detection method, a host-based solution is considered a better solution for monitoring utilising edge computing capabilities. “One alternative and most promising method to network activity monitoring appears to be the monitoring of device resources” (Benkhelifa et al., 2018, p.9).

Hossein Motlagh et al. (2020) describes the use case and enabling technologies to employ IoT devices for improving energy efficiency in the energy sector. Sensor type, actuators, wireless and network technologies for processing information for making decisions for optimal energy consumption. Address IoT in general, but also security issues in general terms related to power production, transmission, and distribution in energy grid systems.

Casola, De Benedictis, Riccio et al. (2019) describes a monitoring system for IoT sensor networks. The authors state that since IDS is IP-based they cannot monitor other types of networks i.e.,

LoRaWAN. A monitoring tool from the company Montimage is used as a use case to support the monitoring of wireless sensor networks (WSN) communication. The Montimage tool is extended to support the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) and is evaluated in a testbed environment using two attack scenarios, namely a [DDOS](#) attack and an [SQL](#) injection attack. The detection is performed using a signature-based network [IDS](#) system. For the [SQL](#) injection attack, the setup does not implement any encryption and solely can detect packet payload in clear text.

The diversity and heterogeneity in [IoT](#) devices have been mentioned as a result of lack of standardisation, however Casola, De Benedictis, Rak et al. (2019) address “ISO/IEC 30141 – Internet of Things Reference Architecture (IoT RA)” as one possible standard to be adopted. However, the “lack of a shared, commonly recognized and adopted IoT architectural and functional vision: the main vendors typically propose their own architecture” (Casola, De Benedictis, Rak et al., 2019, p.1). The authors introduce “a modelling approach to represent both the architectural components of an [IoT](#) system and its security properties” (Casola, De Benedictis, Rak et al., 2019, p.2) to develop an automated process for threat modelling and risk assessment. The automation process could involve similar methods and tools introduced with agile DevOps.

Makhdoom et al. (2019) describes a comprehensive review of the [IoT](#) domain including devices vulnerabilities and attack surface in the layers from hardware to communication to application. The paper gives an overview of different security measures and guidelines to be aware of in the design phase of [IoT](#) use cases and devices to include in an [IoT](#) security framework. The authors provide an overview of threats to the [IoT](#) device, but also preventive and detective measures complemented with security measures and their impact on the [IoT](#) device’s operation. The authors describe adaptive security management as one of several countermeasures and a possible solution by collecting security contextual information and analysing the data. Utilising this to respond by “changing the security parameters such as encryption scheme, authorization level, authentication protocol, level of [QoS](#) available to various applications and reconfiguration of the protection mechanism” (Makhdoom et al., 2019, p.29) of [IoT](#) devices and the network infrastructure. According to Makhdoom et al. (2019) the problem with monitoring of [IoT](#) is based on “Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, may result in implausible auditing and accountability thus allowing attackers to launch further attacks on the systems” (Makhdoom et al., 2019, p.16).

Basir et al. (2019) provides a state-of-the-art overview of enabling technologies within the industry 4.0 domain using fog computing architecture with Industrial IoT ([IIoT](#)) devices to overcome the challenges addressed with less computing power and resources constraint requirements like bandwidth, latency and real-time processing utilising distributed computing and infrastructures. Cybersecurity is raising as one of the main challenges and can by putting security measures on the edge or fog provide enhanced security by enabling stronger encryption near the core [IoT](#) devices as one possible mitigation. But also, infrastructure services including radius protocols for authentication, access and authorisation. When it comes to monitoring [IIoT](#) devices and networks the author suggests using fog computing where “Security issues can be seen on the fog server; it can act as a proxy-server controller” (Basir et al., 2019, p.14).

Hadar and Hassanzadeh (2019) provides an agile methodology with a prototype implementing the perspective on security lifecycle management for an “automatic and agile evaluation for creating a backlog of security issues” (Hadar & Hassanzadeh, 2019, p.331). The backlog is mapped to IT/OT assets to prioritize a work plan with remediation action to be managed by a Security Operation Centre (SOC). Big data analytics is used to analyse data collected from assets including their vulnerabilities, and configuration information to generate attack graphs to predict

possible impacts. The data is complimented with more information from threat intelligence knowledge bases and mapped to business processes with a corresponding risk profile. The authors Hassanzadeh and Burkett (2018) introduce an Industry IoT attack model called SAMIIT to help SOC analysts and SOC processes with classifying events and alerts by mapping them using a machine learning model to bring more context. Another interesting approach to the IIoT attack lifecycle is the defensive OODA loop concept introduced by Boyd (2018) with continuous feedback from each phase in observation, orientation, decision and action (OODA). The “observation, orientation, decision, the action represents what takes place during the command and control (C&C) process” (Boyd, 2018, p.243).

Ferencz et al. (2021) focus on integrating the IoT devices with a proposed architecture to operationalise a SOC to “continuously monitors the devices, centralizing their security oversight and control” (Ferencz et al., 2021, p.245) to reduce the impact of an attack. Design measures are an important factor and the authors state that “Security devices must be designed in a practical, planned manner to ensure the safe and uninterrupted operation of the various protocols, communications and services” (Ferencz et al., 2021, p.247). However, proper insights into what type of assets and vulnerabilities exist in the infrastructure are essential for a SOC to have knowledge about and be empowered to mitigate possible negative impacts and risks for the stakeholders.

Hamad et al. (2020) provides a structured approach by addressing security issues, privacy, and trust for realising an internet of “secure” things. By pointing out several security threats faced by IoT devices and possible countermeasures due to resource constraints on such devices i.e., micro-controllers with suggested design measures. The authors have provided an overview of different challenges divided into different architecture layers where they state that the “challenge is to build less vulnerable standardized, secure operating system for the constrained devices that can provide all of the security and privacy services” (Hamad et al., 2020, p.1373). A proposed solution according to the authors can be to outsource the computational load to the edge of the network and let the IoT devices “borrow some computational power from edge devices to do partial encryption/decryption during uploading/downloading data” (Hamad et al., 2020, p. 1377). However, IoT security in operating systems like Ubuntu Core, TinyOS, RIOT OS and similar should support security services, but “most of these common operating systems are incapable of addressing the needed security requirements for IoT infrastructures” (Hamad et al., 2020, p.1373).

According to Tagarev and Sharkov (2019) modern technology stacks incorporate compute, storage and analysis capabilities for security monitoring of “decentralized, distributed, networked, interoperable compositions of heterogeneous and (semi)autonomous systems and/or elements” (Tagarev & Sharkov, 2019, p.9). When discussing the perspective on “system of systems” the authors define a new concept by introducing a distributed Systems of Security Operation Centre, SoSOC, where the “resulting complexity of the system of systems is rising, increasing the necessary human and computational efforts to understand risks and find a portfolio of measures that is affordable and minimises the overall risk” (Tagarev & Sharkov, 2019, p.9). The concept behind the SoSOC is the “interoperability and interdependencies” and “operations and security” layer which should address not only the sharing of threat information between SOCs, but also the context triaging of the resulting knowledge from people, process, and technology perspectives.

The Colelli et al. (2019) authors have developed an IDS solution based on signatures and anomalies using deep packet inspection for protecting the communication channel for legacy OT sensors and actuators. The “Fog Intrusion Detection System (FIDS) preserves the ability to identify a cyber-attack and provide the IT, in a safe way, data on the status of the process” (Colelli et al., 2019, p.445). The device is placed in the convergence zone as a bastion host between IT and OT networks and is specially adapted and hardened for the purpose. The FIDS device does not propagate control

commands towards the legacy IoT devices. However, the FIDS device only reads the values from the sensors and sends them using the MQTT protocol. The authors touch upon the monitoring perspective and the possibility to forward information using the MQTT protocol where “the device is able to report OT network anomalies to the Security Operation Centre (SOC)” (Colelli et al., 2019, p.446).

Q. Qiu et al. (2021) suggests better alignment of security standards in the massive deployment of IoT devices in the era of 5G. The authors investigate security requirements and measures for the following layers defined as (1) sensor control, (2) network and transmission exchange, (3) application and services, and (4) security management and operation. Cyber security and monitoring are research fields when dealing with IT-related components. However, the IT and OT is merging, and requires better insight into the IoT devices and network behaviours when defining new security measures for monitoring. According to the authors they foresee that introducing edge computing is a key component for improving IoT security to “provide security guarantee for the smooth operation of IoT services” (Q. Qiu et al., 2021, p.8). “Cyber security monitoring is of great significance to the security of the IoT, and the role played by edge computing techniques is indispensable” (Q. Qiu et al., 2021, p.8).

Bertino (2019) introduce an IoT security lifecycle approach consisting of four contextual phases to address IoT security, namely to (1) prepare and prevent, (2) monitor and detect, (3) diagnose and understand, (4) react, recover and fix. Because of IoT heterogeneous characteristics “managing security for very large numbers of heterogeneous devices may not be always humanly possible” (Bertino, 2019, p.196) and suggest that IoT networks with edge compute technology could provide capabilities to “continuously monitor the system of interest in order to detect attacks or anomalies that may be indicative of attacks.” (Bertino, 2019, p.197). In addition, the author suggests that IDS should be implemented on the edge of the sensor network and have support for several communication channels i.e., ethernet, wireless networks, Zigbee, Z-wave, and Low-Power Wide-Area Network (LPWAN). Data collection with diagnostics parameters from the IoT device will provide better insights to detect attacks and the author suggest collecting link quality indicator (LQI) and the received signal strength indicator (RSSI) from IoT devices. According to the author, “A real-time anomaly detection system is crucial for enabling quick responses to attacks.” (Bertino, 2019, p.198).

2.2.5 Tools, assets and skills

In general, having tools available to use when handling a cyber incident is essential and of high importance to be more robust to handle the impact of cyber-attacks. But with tools available also comes the need for skills and competence in using them. Developing effective incident handling procedures requires hands-on training using forensic tools and how to execute the chosen response. Important factors in incident response are – time to detect, time to respond with an effective defence strategy and time to recover business services. The most important is to know your assets, the functionalities, and the capabilities which IoT devices provide within the value chain of IoT and the business.

The knowledge about existing threats and vulnerabilities to the IoT device and network gives a context that is relevant to develop risk profiles that could provide information to make better incident plans.

A detection mechanism with dynamic risk profiling that could identify and map network traffic to specific attack types is something that is available through the use of Intrusion Detection Systems (IDSs).

The **SOC** should identify and develop incident response plans; using threat hunting, and detection patterns and enabling cross-organisation coordination, communication, and collaboration; arming analysts with technologies that enable them to make accurate decisions and act quickly.

2.2.6 A summary of the state of art literature

In this semi-structured review of the literature on **SOC** and **IoT** monitoring, we have analysed the literature, conducted using the snowballing method to give a state-of-the-art perspective on the current development and status of the **IoT** domain and the challenges. We have identified from the literature that the lack of implemented security in the design phase and security measures in the **IoT** domain is prevalent. There is less information in the literature about how to address and solve these security challenges.

The challenges are still severe, and the heterogeneity and amount of **IoT** devices to collect information through **IoT** device monitoring metrics (**CPU** load, memory consumption, etc.) seem to be less focused. However, the use of machine learning algorithms and methods has been discussed as a better solution when dealing with **IoT** heterogeneous to distinguish between types of devices and behaviours. Security operation centres (**SOC**) have a central role and interest in the monitoring of **IoT** devices and networks. However, there seems to be more focus on the network infrastructures in conjunction with edge and fog services for anomaly detection and less on the actual **IoT** device behaviour and performance metrics. Best practices for fleet management tools and services with integration to **SOC** were limited in the literature. Nevertheless, there is a need for greater visibility of the assets both from **IoT** and **OT** devices. But with the slow adoption of **IoT** standards the different vendors and solutions in the diversity with limited information about how to optimally monitor these **IoT** devices. Seen from the perspective of a **SOC** there are still some basic mechanisms that need to be addressed and implemented when a successful cyber-attack has happened – the ability to detect, respond and mitigate security incidents in time is crucial.

The DevSecOps model is an interesting approach that could address **IoT** security and device management with the integration of security practices and software delivery models to address these challenges. However, the **SOC** seems to be a rather new component in the DevSecOps model, and should be investigated further, if the current toolset, methods, and data from the **IoT** domain could be a part of a new **SOC** operating model in the future.

Chapter 3

Methodology

In this chapter, we introduce a qualitative methodology approach and an exploratory research design to find answers to our research questions. In this study we will seek information about existing practices and if SOC's are aligning with the emerging number of different IoT systems by conducting interviews with security professionals. With an exploratory research approach, we want to explore and identify challenges and problems, techniques and methods along with the organisational processes that potentially prevent the SOC's abilities and awareness of IoT in security monitoring. We will describe this through the use of different thematic areas that would help us to identify, categorise and validate the findings from conducting interviews. We will introduce and use thematic analysis as a method to identify current practices, and how and why SOC's should focus more on IoT devices and their eco-systems for security monitoring.

3.1 Research design and methodology

The state of the art revealed a lack of device monitoring parameters for security monitoring, important for a SOC's ability to detect and respond to cyber-attacks. In this study, we will use an exploratory research design to explore the relationships between the increasing number of different IoT devices and ecosystems, and SOC's preparedness and awareness of such devices. "Exploratory research is a methodology approach that explores research questions that have not previously been studied in depth." (George, 2021). Using an exploratory research approach lets us use existing research to identify new perspectives on SOC organisational functions and IoT devices as an increasing vector of surrounding threats and vulnerabilities.

Our working hypothesis is based on the assumption that *SOCs are facing many different challenges in the establishment of a unified security monitoring process of IoT assets; caused by factors of closed ecosystems or vendor lock-ins, cheap IoT hardware and poor software design with complex management and software deployments.* SOC's often lack insights and an up-to-date overview of the system landscape with regard to IoT assets. By exploring this situation, we will identify and gather information from real systems and use cases that are in production in different organisations today, where they already are focusing on security monitoring. We are exploring this from the perspectives; including those of a vendor, a customer, government and public sector stakeholders, and from the point of view of a critical infrastructure owner.

There is a need to explore and identify new practices and methods for a broader uptake of IoT systems for security monitoring (European Union Agency for Cybersecurity., 2022, p. 36). With the aim to get better insights and knowledge about the complexity of IoT monitoring, with systems that

have limited resources, criticality and capabilities for detection, and incident handling of security events within security- or operational teams.

By using different methods from the qualitative research we want to both identify the challenges that need to be overcome to improve SOC's preparedness for more detailed monitoring of IoT systems and explore different approaches and best practices that exist today. To find answers to the research questions we conduct semi-structured in-depth interviews with security professionals from different sectors in Norway to bring forward more knowledge about existing IoT systems, and the real problems and practices that SOC's are facing today.

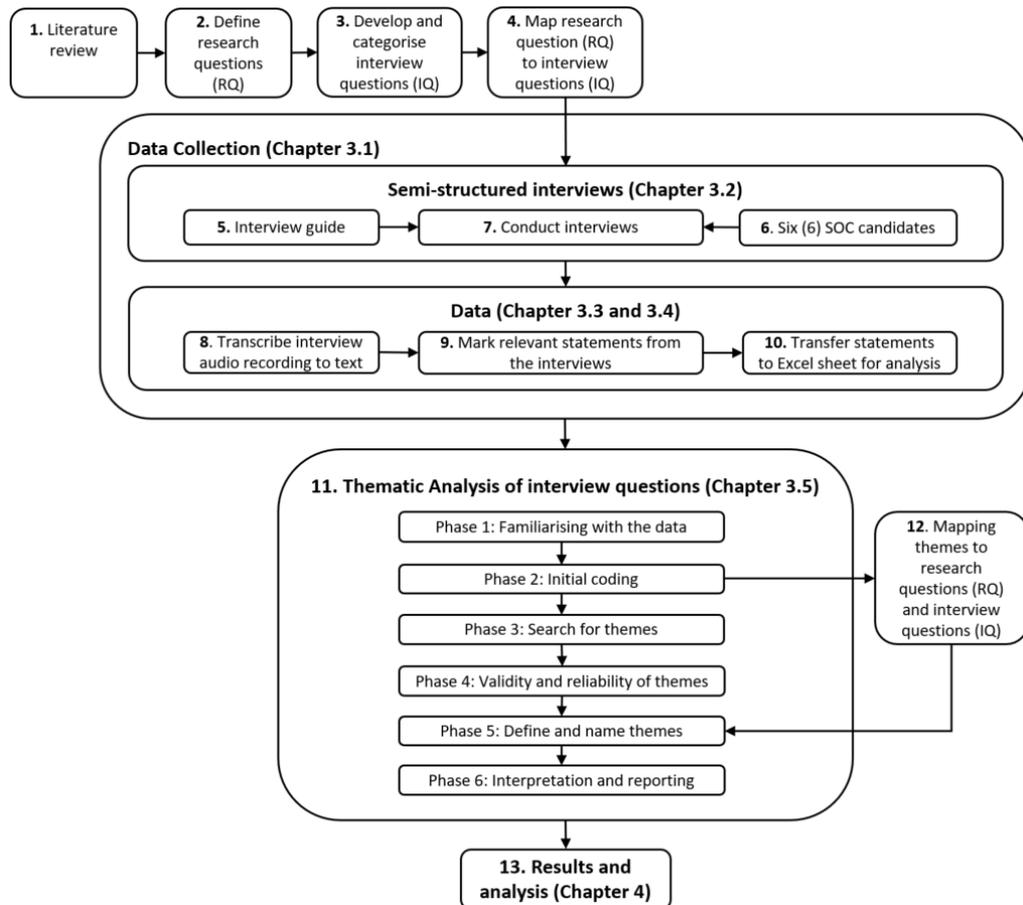


Figure 3.1: The methodology

3.2 The semi-structured interviews approach

The objectives of using semi-structured interviews as a data collection method was "to gain a rich understanding" (Kallio et al., 2016, p. 2955) and a better overview with deeper insights about how IoT devices and different systems typically are handled by a SOC (Security Operation Centre), or a CERT (Computer Emergency Response Team), or IRT (Incident Response Team) in different organisations. What types of challenges exist today and are IoT devices in the scope of SOC's assets for monitoring and detection? One of the main questions would be to identify how IoT devices should be monitored and operated for better detection of security events or anomaly activities seen from the SOC perspective.

Based on the insights and findings from the state-of-the-art literature review, and the three main research questions, a total of 13 open-ended questions were developed. In addition, for each question, additional one to four follow-up questions were also developed. With the use of open-ended questions, we hope to find more answers about what, how, and why. The questions were further categorised into four main topics; background information about typically (1) business drivers, (2) how to do IoT management, (3) how to do monitoring and detection of security events, and lastly (4) how should SOCs be organised to handle security incidents from several different IoT devices and infrastructures.

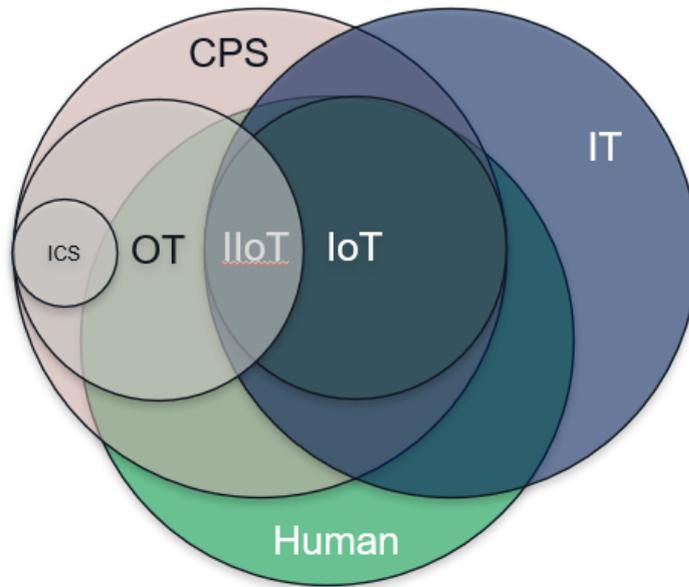


Figure 3.2: The IoT domain and research perspectives

To answer these interview questions, we wanted to explore the perspectives from within one organisation by asking the interview candidates about their experiences and opinions as the subject-matter-experts from working and operating in the IT/OT field.

We have developed the following interview guide with open-ended interview questions (IQ) to explore the domain of SOC and IoT:

Business drivers

- IQ1: To what extent would you say that businesses(s) use or have IoT devices?
- IQ2: How important (critical or dependent) would you say IoT is to your business?
- IQ3: How do you think IoT has or will impact your corporate or enterprise network?

IoT management

- IQ4: Do you distinguish between IoT, Industry-IoT and Operational Technology (OT) devices in how you handle and operate these devices/systems?
- IQ5: What would you say are the challenges with different IoT systems today?
- IQ6: What type of security barriers/mechanisms are necessary to protect such IoT devices?

Monitoring and Detection

- IQ7: How should IoT devices be maintained and monitored?
- IQ8: How do IoT devices log and report?
- IQ9: Is edge computing or a central gateway for monitoring IoT devices something that is in use today?

Security Operation Centres

- IQ10: How do you think IoT devices should be introduced to a security monitoring SOC team?
- IQ11: How do you think SOC should be organised for optimal monitoring of IoT devices?
- IQ12: In what way is the organisation of the SOC influenced by the business objectives?
- IQ13: What type of SOC operating model should be used for IoT?

3.3 Planning the interview process

The interviews were conducted both physically and digitally using Microsoft Teams¹ as the video-conference service. The questions were asked and supported by a PowerPoint presentation with a brief introduction to the objectives for the research along with the research problem - "How should SOCs monitor IoT assets for effective detection and response?". In addition, the three main research questions were presented for the candidates to give more context and understanding during the interviewing process.

Information about the interview process (Appendix A) was given and the candidates signed a consent form (Appendix B) describing how the study will be conducted with the aim for the candidates to approve their participation, recording of audio and using the information the candidates shared during the interviews. The data management plan and the approval of starting the interviews were in line with laws and regulations. The data management plan was handled by NSD - the Norwegian Agency for Shared Services in Education and Research. The audio recording was based on using the secure Diktafon application integrated with Nettskjema.no services for the safe and secure storing of sensitive information. We were interested to explore and find more knowledge about the candidate's opinions and experience from within the research field. The name of the organisation, to which the candidate belongs, was used to categorise and identify the different responses. Each interview took about 45-60 minutes and was conducted and completed during the autumn of 2022. We asked seven different SOC candidates in total, and from those seven, we got six positive feedback with a commitment to their participation. The six SOCs were from businesses within the Norwegian security community.

It is also important to mention and take into account each participant's risk of exposing sensitive information about vital or critical assets from their business, naming specific customers, current status and ongoing investigations or specific IT/OT components and infrastructures.

¹Microsoft Teams <https://www.microsoft.com/en-us/microsoft-teams/group-chat-software>

3.4 Qualitative data collection

The data collected from the semi-structured interviews were based on manual transcription from audio recordings from each interview. The transcribed information and the individuals were anonymised by only using the company name and a respondent's ID (R1-R6) for identification when tracking quotes, opinions and narratives. No personal information from the interviewed candidates was to be exposed and should be aligned with the signed agreement.

3.5 Analysis methodology

In this research, we will use thematic analysis to identify any patterns or themes within the data set that could be relevant (Braun & Clarke, 2021). Braun and Clark introduce a step-by-step guide for doing a thematic analysis of the interview data. The phases in a thematic analysis will follow six steps, with the use of iteration between the phases (Braun & Clarke, 2006, p.87).

1. **Phase 1. Familiarisation of the data:** The first step is to familiarise ourselves with the data and transcribe it if necessary. Also reading through the transcribed text several times and noting down initial ideas.
2. **Phase 2. Initial coding:** The next step is to identify initial coding using a systematic approach across the entire data set.
3. **Phase 3. Search for (generating) themes:** Collect data relevant to each theme.
4. **Phase 4. Validity and reliability (review) of themes:** Check if themes relate to the coding and generate a thematic map of the analysis.
5. **Phase 5. Defining and naming themes:** Refine the specifics of each theme and generate clear definitions and names for each theme.
6. **Phase 6. Interpretation and reporting:** The final analysis of selected extracts and the relationship to research questions and the literature review.

According to the method of thematic analysis (ibid), we have followed the phases for analysing the current data set consisting of six interviews. The process involved carefully listening to the audio recordings and transcribing each interview to text as precisely as possible. In addition, it is important to read the transcribed interviews carefully several times to get an impression of what type of valuable information or relevant text relies on in sentences and statements. The text of relevance and importance in the transcripts was highlighted for later use. The analysis of the text was an important part to gain insight into how the participants answered each question. All the highlighted text consisting of statements and answers was further transferred into a spreadsheet for categorisation. This process involved us analysing each interview question with initial codes and themes. In Appendix G we provide a detailed overview of the results and the process of using thematic analysis with phases from 1 to 5.

3.5.1 Phase 1 - Familiarising with the data

We walked through the data set with the aim to develop and identify an initial coding schema. The coding schema was further developed to find common factors for familiarising with the data.

We analysed each research question with a topic or theme that would reflect a common ground or relationship between the research questions and the interview questions. The following initial themes in Table 3.1 were identified by analysing the research questions and extending the theme with mappings to the corresponding interview questions identified by a circle marker. The intention of this was to help and guide us through the data set using the process of thematic analysis to identify which RQ each interview question would answer.

Table 3.1: Topic mapping schema with initial coding and answering the RQs through IQs.

RQ	Theme	Business drivers			IoT management			Monitoring and detection			SOC			
		IQ1	IQ2	IQ3	IQ4	IQ5	IQ6	IQ7	IQ8	IQ9	IQ10	IQ11	IQ12	IQ13
RQ1	Challenges	-	-	●	-	●	-	●	-	-	-	●	-	-
RQ2	Information	-	-	-	●	-	●	●	●	●	-	-	-	-
	Technical	-	-	-	●	-	●	●	●	●	-	-	-	-
	Devices	-	-	-	●	-	●	●	●	●	-	-	-	-
RQ3	Organisation	-	-	-	-	-	-	●	-	-	●	●	●	●
	Background information	●	●	●	-	-	-	-	-	-	-	-	-	-
	Assets	●	●	●	-	-	-	-	-	-	-	-	-	-
	Threats	●	●	●	-	-	-	-	-	-	-	-	-	-

3.5.2 Phase 2 - Initial coding

After transcribing all audio recordings from the interviews to text and familiarising them with the data as described for phase 1, we identified eight initial themes or topics. The identification of the initial coding and themes was found by mapping the relevance (subjective meaning) of each answer to an IQ with the corresponding RQ throughout the entire data set. The initial themes were: "challenges", "information", "technical", "devices", "organisation", "background information", "assets" and "threats".

Phase 2 of the process was to code the answers using the respondent's ID as identification in front of every sentence or statement. We provide an example of such a statement from respondent 1 using the following format here: "R1: challenging to monitor endpoints and sensors".

3.5.3 Phase 3 - Search for themes

During the identification of themes, we searched through the whole data set as described for phase 3. This process represents a holistic approach, where we try to find answers to the IQ's relevance for each theme. To guide this process, we asked ourselves "what" is the problem, "why" is this relevant, and "how" should we approach and address the issues found in the interviews? This process appeals mainly to the investigator's own subjective interpretation of how we mapped different statements to these themes. However, during the analysis, we want to highlight the process of conducting a thematic analysis in light of the validation and reliability of chosen themes and present statements as results from the interviews.

3.5.4 Phase 4 - Validity and reliability of initial themes

The process of categorising statements and quotes is not a straightforward task and requires an iterative approach and re-reading all the statements for each IQ to identify if the theme will fit the purpose. According to phase 4 (Braun & Clarke, 2006, p. 91), initial themes should be refined if it

becomes evident that it does not apply as a theme or be too broad in the sense of the meaning. In the following section, we describe the eight initial themes in more detail when familiarising with the data set.

In phase 4, we address the validity and reliability of each theme through review. Heale and Twycross define validity "as the extent to which a concept is accurately measured in a quantitative study" (Heale & Twycross, 2015, p. 66).

What would be a valid theme in this phase and context? The intention of naming themes would be to give them a name that is fruitful. Themes are defined to describe "something important about the data in relation to the research question, and represents some level of patterned response or meaning within the data set." (Braun & Clarke, 2006, p. 82). In relation to this statement, we have made a decision about how each of the themes was mapped with respect to the RQ as described in our methodology chapter and table 3.1. According to Heale and Twycross reliability "relates to the consistency of a measure" (Heale & Twycross, 2015, p. 66). It is important to notice that every theme could be applicable to several interview questions (IR). However, we have chosen where this should be of significance when we mapped the relation between RQ and IQ. When considering the reliability of each theme at this level we should also consider how 'accurately' the themes "reflects the meanings evident in the data set as a whole." (Braun & Clarke, 2006, p. 91).

To validate if a theme is appropriate, Braun and Clarke provide two levels of guidelines for reviewing and refining themes. If we look at the first level "involves reviewing at the level of the coded data extracts" (ibid) and level two "involves a similar process, but in relation to the entire data set" (ibid). This means, that our data set should be validated so that each "themes should cohere together meaningfully, while there should be clear and identifiable distinctions between themes." (ibid).

Reliability and validity

In general, we consider all statements in relation to the themes for the reliability and validity of each participant's answers. These answers should therefore be considered as a snapshot both in time and in the context of a semi-structured interview setting. To validate the statement's validity with the corresponding themes, we have created a simple scoring system based on the number of SOCs provided an answer, with the thresholds and a circle representation given in the frequency Table 3.2.

Table 3.2: Validity scoring system

Score	Number	Representation
None	0	
Low	1	
	2	
Medium	3	
High	4	
	5	
	6	

Using this scoring system, we validated the statements and presented each category for the IQs through its: business drivers, IoT management, monitoring and detection, and SOC. During the walk-through, we followed a strict process and used each statement where the theme mapping corresponded with the IQ, providing us with answers to the IQs. In Appendix C we have provided an overview of the qualitative data analysis of all the statements provided by the respondents according to the frequency table.

In the next sections, we provide more detailed information from the answers to the IQ and presented the findings from the interviews.

Challenges

With the theme "challenges" we searched for existing problems that would give information about what the obstacles or barriers in different situations would be, but also the impact on the "why" by finding answers that potentially block the adoption of i.e. new methods, organisational factors, best practices, or technologies. We have considered this theme to be valid for RQ1, where we seek to find answers about the problems in security monitoring, or organising and operating IoT systems in practice. However, the theme would be relevant for many of the other themes mentioned as well, if we think of "challenges" wider, i.e. organisational challenges or technical challenges. To validate if "challenges" were an appropriate theme we use the guidelines from level one by Braun and Clarke to go through all the statements and quotes, and verify and sense-making if we can relate it to this theme. The different statements were quite easy to identify because of their "meaning". Here are five examples of statements (within the entire data set), one statement from each SOC, that exemplifies the validity of the meaning and relevance of the theme "challenges":

"...for a SOC, it is challenging to keep track of everything..." (R1)

"...lack of insights makes it difficult to establish security monitoring and do threat hunting..." (R2)

"...the biggest challenges - discovering abnormal things that are happening..." (R3)

"...it is not so easy to streamline the operation of such systems... it is often tailoring and different systems that can be a big challenge... both with expertise and resources..." (R4)

"...IoT devices that has no security in the component structure in relation to the OSI layer..." (R5)

"...very few have the opportunity to send the logs you actually need..." (R6)

We have considered the validity of "challenges" to be a suitable theme based on the sentences mentioned above how well it fits and their relevance. We considered the validity using Braun & Clarke's level two guideline, the entire data set with the theme for every statement.

When counting up all the "challenges" found in phase 3, covering the entire data set, we have 118 different statements. This was the highest number of statements in relation to the other themes. However, this high number gave us a grounding of the fact that SOCs are facing many different challenges in the context of IoT.

Information and data

The theme "information and data" is a category meant to describe the "what" through narratives, use cases, functions or information about i.e. monitoring parameters that could give us knowledge of what is currently in the scope for IoT security monitoring. The validity check of the theme "information and data" involves considering this in relation to the RQ2 where we explore "what" type of information is collected from IoT devices. The theme gives us a strong identifiable distinction between the theme and RQ2. The theme has 83 sentences and statements that figuratively speaking have been identified through smaller narratives or stories from within the data set. In the examples below we will share two statements where we have interpreted what type of information would be relevant for the theme (level one) and give us answers for RQ2 when considering the entire data set (level two).

"...information can also be obtained by listening on the network and then there is less risk of affecting the PLC as well..." (R2)

"...heartbeat and netflow is essentials..." (R5)

The theme "information and data" have its validity for relevance when considering and sense-making the data set with RQ2.

Technical

The "technical" theme describes technical aspects and information about networks and infrastructures, type of products, methods in use and technologies that are relevant. This could address both the "what" and "how", but also more details about the technical level when describing different architectures, infrastructures, and standards within IoT management and security monitoring. This theme has a strong relation to RQ2. The interpretation of the technical aspects we have considered and highlighted the statements below. The statements describe three examples of relevance to architecture design principles, infrastructures, and the importance of having logs available for security monitoring.

"the newer systems have more built-in security where I would say they are more segmented in the way they are designed" (R1)

"...between level 3.5 and 4 it is two-factor, logging, jump hosts, we build up our jump hosts every other day so that persistence will be almost impossible to achieve..." (R2)

"...log analysis will be... and is increasingly important..." (R3)

The theme "technical" have 104 different statements when we considered the entire data set. This indicates that the theme has good validity for its relevance.

Devices

Devices can be described as typical devices or endpoints that are vital to the data value chain. We consider the importance of connectivity and characteristics that could describe the type of sensors and actuators. The theme "devices" had a relation to RQ2 and is valid if we can identify types of devices and typical sensor data through the statements. However, this theme scored low with a total number of 23 statements considering the entire data set. So how should we validate "devices" as a theme? In general, during the interviews, there were shared fewer technical details about IoT devices and device types by the participants. It was harder to identify and directly relate some of the statements to this theme. This should be interpreted that the participants had trouble talking about or relating to IoT devices. We had to interpret these statements more indirectly when considering the participant's answers. The following two examples of statements below have relation to the theme "devices".

"...mostly wirelessly for the simplest IoT devices..." (R5)

"...must be live asset data..." (R6)

This would of course not invalidate the theme entirely. IoT devices were a central component of this study and are considered to be a valid theme. The theme scored lower on validity for its relevance with respect to the data set. There were statements from other themes that indicated a stronger relevance for the "devices" as a theme. Both "assets" and "technical" have some statements that could identify device types.

Organisation

Organisational factors were important and played a central role in the operation of a SOC. These factors were typical aspects of human operators, culture, communication, processes, environment or structures that had an impact directly and indirectly on how a SOC should be operated. The theme "organisation" have a strong link to RQ3 where we seek knowledge about the inner life of a SOC. We would also relate competence as part of this theme. We found 70 statements in relation to SOC and IoT, considering the entire data set in relation to the "organisation" theme. We give three examples of "organisational" statements below that validate the need for such a theme.

"...larger companies have preferably their own personnel that would like to handle the network part themselves... so that the data does not end up astray or other things..." (R6)

"...very separate in terms of personnel and separate between IT and OT..." (R2)

"...plan, implement, operate and improve – getting it into the normal cycle of the SOC..." (R5)

Background information

General background information should give us more insight and context by seeking information about the "why" and "what" when we consider statements on how a SOC should be operated in relation to RQ3. The theme "background information" should provide us with information categorised with typical business drivers and with 45 different statements when considering the entire data set. The validity of the theme "background information" had a strong relation to the concepts of SOC and the IoT domain. Example statements include:

"...OT has a more risk-based approach with 62443 versus IT with typical ISO 27001..." (R2)

"...several sectors that have trial projects on IoT devices..." (R5)

"...there are buildings that are of critical value for housing a function..." (R5)

Assets

Assets are known to describe something valuable that is vital for a party. "The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns." (NIST, 2023) The theme "assets" maps to the business drivers as an important object to identify in relation to RQ3 where we searched for the "why" through the data set for statements describing risks or criticality.

The validity of the theme "assets" depends on how well it links to RQ3 and the relation to IoT systems in general. However, the theme "assets" score the lowest with only 18 statements. Nevertheless, we have mapped several statements with a strong relationship to assets, as mentioned in the examples below.

"...in relation to criticality, I would say that it is different in the various sectors where buildings are perhaps the most critical..." (R5)

"Within OT, everything from gas control to the safety systems are OT systems that are normally connected to the network. So without the OT systems, the whole company stops!" (R2)

Threats

The themes "threats" in a broader meaning, would be anything that had a negative impact or can cause an incident. Concerning the theme "assets", threats can be further categorised into two subcategories, malicious and non-malicious threats, where threats potentially negatively impact an asset. We, therefore, distinguish between intended and unintended (unexpected) events. However, the theme is valid if we can find statements that fit the description. Searching through the data set for statements we found 38 statements. Considering the statements, we have a strong relationship to the vulnerabilities, practices and techniques that is relevant to validate this theme. Vulnerabilities have the potential to reduce or degrade the value of an asset. Example statements include:

"...there will be vulnerabilities on a PLC where you can do one thing or another with a buffer overflow..." (R2)

"...the actors who have such resources are good at building malware to knock out such systems..." (R3)

3.5.5 Phase 5 - Refining and naming the themes

In phase 5 of the thematic analysis, we refined the themes to be more specific in their description by generating clear definitions and names for each theme. When defining and refining the themes "we mean identifying the 'essence' of what each theme is about" and "determining what aspect of the data each theme captures" (Braun & Clarke, 2006, p. 92).

The eight initial themes emerged into eight more specifically named themes during our analysis. We have made minor syntactic changes to the theme names, without moving or rearranging the data. The refined themes are high-level SOC factors, that should be addressed and considered in the process of preparing and scaling a SOC for security monitoring of IoT devices. The themes are described and rearranged in Table 3.4.

Table 3.3: Refined themes

Initial theme	Revised theme	Theme description
Challenges	Challenges	Challenges describes something new and difficult that would require a great effort to achieve (Collins, 2023). In this context, challenges represent something difficult that prevents a change in existing practices, methods or in the adoption and use of new technologies.
Information and data	Metrics, events and alarms	This theme describes technical security parameters, methods or use cases that provide existing or new knowledge in IoT monitoring. Metrics are quantitative measures of relevance to improving the detection of security events.
Technical	IT and OT infrastructures	The "technical" theme describes technical aspects and information about the underlying IT and OT infrastructures and networks in use and the relevant technologies. After refining the "technical" theme, we find it to be more descriptive by renaming the theme to describe "IT and OT infrastructures".
Devices	Devices	The theme "devices" is defined as electronic equipment that is vital to provide data and values from sensors and actuators through connectivity with process characteristics of the data. Devices are the enabler for transferring sensor values utilising the data value chain (OpenDataWatch, 2018).
Organisations factors	Human and organisational factors	The "human and organisational factors" theme describes the interactions between system components and humans when considering the behaviour inside an organisational unit or with external business suppliers and partners.
Background information	Background information	This theme provides historical information or situations that would describe common problems or circumstances in relation to the business.
Assets	Assets	The theme "assets" describes anything that would be of value which enables an organisation to achieve its business goals and purposes.
Threats	Threats and vulnerabilities	The theme "threats" is extended to include "vulnerabilities" which would be a better description related to the statements. "Threats and vulnerabilities" are tied closely together and are complementary in the sense of meaning and relate stronger to the statements.

Table 3.4 presents the revised topic mapping schema from Table 3.4 below is updated to support the process of further analysis with mappings to RQs and IQs for references.

Table 3.4: Topic mapping schema with the **refined themes**.

RQ	Theme	Business drivers			IoT management			Monitoring and detection			SOC			
		IQ1	IQ2	IQ3	IQ4	IQ5	IQ6	IQ7	IQ8	IQ9	IQ10	IQ11	IQ12	IQ13
RQ1	Challenges	-	-	●	-	●	-	●	-	-	-	●	-	-
RQ2	Metrics, events and alarms	-	-	-	●	-	●	●	●	●	-	-	-	-
	IT and OT infrastructures	-	-	-	●	-	●	●	●	●	-	-	-	-
	Devices	-	-	-	●	-	●	●	●	●	-	-	-	-
RQ3	Human and organizational factors	-	-	-	-	-	-	●	-	-	●	●	●	●
	Background information	●	●	●	-	-	-	-	-	-	-	-	-	-
	Assets	●	●	●	-	-	-	-	-	-	-	-	-	-
	Threats and vulnerabilities	●	●	●	-	-	-	-	-	-	-	-	-	-

The circle marker indicates which theme an IQ answers. The themes are further grouped to which RQ they answer. For example, the category Business drivers (IQ1-IQ3) maps to the four themes "challenges", "background information", "assets" and "threats and vulnerabilities". The other themes are not relevant to this category.

Chapter 4

Results and analysis

In this chapter we present phase 6 of the thematic analysis with the results from the interviews.

The semi-structured interviews were conducted and supported by an interview guide (Appendix A) of the research problem and our three main research questions. In Figure 4.1 we give an overview of the interview period in time and the order of the interviews with respondents (R1-R6).

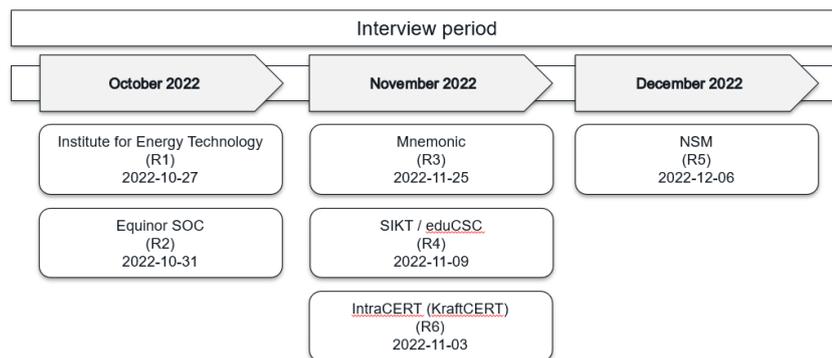


Figure 4.1: The interview process in time

The selection of interview candidates or subject-matter-experts (SMEs) was selected based on the author's contacts within the security community and the knowledge about the candidate's experiences within cybersecurity, security operation, incident response and IT/OT. We contacted each candidate individually either by direct contact or by contacting the company sales representative for help on identify the correct and available resource that could participate in the interview. The selection group was made based on a total of seven inquiries to companies and candidates about their participation, where they also have a relationship with SOCs, Computer Emergency Response Teams (CERTs) or Incident Response Teams (IRTs) in Norway. We got a positive response from six of the seven SOCs for participation. After establishing contact with the right individual expert and confirming their commitment to participate in the research project, the next step was to schedule meetings for the actual interviews. There was only one representative from each SOC that participated in the interview.

The interviewed participants in Table 4.1 show each representative from Norway's different public- and private organisations.

Table 4.1: Interview candidates affiliation

ID	Company name	Description	Type
R1	IFE SOC	"At Institute for Energy Technology (IFE), we build bridges between research, education and industry. We have extensive infrastructure and full-scale laboratories where theoretical models are transformed into commercial activities. IFE has unique expertise and systems within radiation protection and environmental monitoring of radioactive and chemical emissions. This makes us an important partner for companies that want to research, develop and produce new solutions for renewable energy and medicine using radioactive sources." (IFE, 2023)	Research institute
R2	Equinor SOC	"Our onshore facilities in Norway include activities in crude oil reception, gas processing, refining and methanol production. We also have operational responsibility for the world's most extensive subsea pipeline system for the transportation of gas. In addition, we have seven supply bases along the coast that provide important knock-on effects in their local communities." (Equinor, 2023)	Energy production
R3	Mnemonic	"mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. mnemonic is a cybersecurity service provider offering clear answers and pathways to complex security challenges." (Mnemonic, 2023)	Vendor supplier
R4	SIKT eduCSC	"The Cybersecurity Center is the sector-specific response team for Norwegian research and higher education. We deliver a range of security services, and are the focal point for security expertise in the knowledge sector." (SIKT, 2023)	CERT
R5	NSM	"NCSC is a part of the Norwegian Security Authority (NSM). We are Norway's national cyber security centre and home to the national CERT; NorCERT. We handle severe computer attacks against critical infrastructure and information. Our mission is to enhance Norway's resilience in the digital domain." (NSM, 2020)	Government
R6	IntraCERT (KraftCERT)	"InfraCERT optimizes securing of process control systems for the power industry. We update our customers about relevant vulnerabilities and threats, so that they will be able to detect and defer digital attacks." (KraftCERT, 2023)	CERT

4.1 Analysis of interviews

The value of using thematic analysis depends on how we interpret and use the identified themes. Maguire and Delahunt argue that the value and benefit of "thematic analysis is to identify themes, i.e. patterns in the data that are important or interesting, and use these themes to address the research or say something about an issue." (Maguire & Delahunt, 2017, p. 3353). We have now defined our initial themes and validated them for use on the data set. In phase 6 of thematic analysis, we tell the story (Braun & Clarke, 2006, p. 93) of the data through the use of validated statements by the scoring system.

The interviewed participants represent different sectors and business areas as mentioned in Table 4.1 and each of them was answering on the questions in the context of their experiences, business needs and operation. This gives a wider spectrum and background information for the provided answers. The questions were asked in sequence as numbered. When conducting a semi-structured interview, we asked follow-up questions to narrow down to more specific areas of interest that related to IQs. Each IQ was developed with additional questions to help the participants to find a relevant answer to our questions. An example would be when asking IQ1 "To what extent would you say that business(es) use or have IoT devices?" regarding the identification of the business drivers. Here the participants sometimes had trouble relating themselves with what they do in their daily operations to business goals or activities. A typical follow-up question to help them on the way was to ask if such IoT device exists or is in operation today, or if the business unit is aware of having such devices in their business. Another approach that was used during the interviews was to ask if they can provide examples. In an interview setting, we often get richer answers from the participants that also would give answers to other questions that we would ask later.

4.1.1 A SOC's monitoring approach towards IoT ecosystems

Based on the different answers provided during the data collection, we have mapped each interview participant to the type of system domain they identified themselves with as their focus areas. In Figure 4.2 we represent the mapping of the IoT domain VENN-diagram for each SOC's focus area. There are overlaps with several other domains, but in Figure 4.2 we present three main focus areas, namely the cyber-physical systems (CPS), information technology (IT) and the human. Having a holistic view of the perspectives of people, processes and technology is equally important to address the complexity of IoT systems. With people or human aspects, we address competency, knowledge and awareness. The process perspective addresses the complexity of the system of systems and the advances in connecting cyber-physical systems using the technology perspective with connectivity and interoperability of systems and devices. These perspectives are often referred to as success factors where the focus was to find a good balance between them to drive for the action of change and digital transformation in organisations (Simon, 2021).

SANS Institute defines a Security Operation Centre (SOC) as "a combination of people, processes, and technology protecting the information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects." (Crowley & Pescatore, 2018). Nevertheless, the SOC should play a central role in minimising the gap and bringing more knowledge and uptake of IoT devices within security monitoring.

It is important to clarify some of the differences between IoT, IIoT and OT devices and how they were used and can be monitored. The Internet of Things or IoT is used as a collective term for different types of devices, which includes both the Industry Internet of Things (IIoT) and to

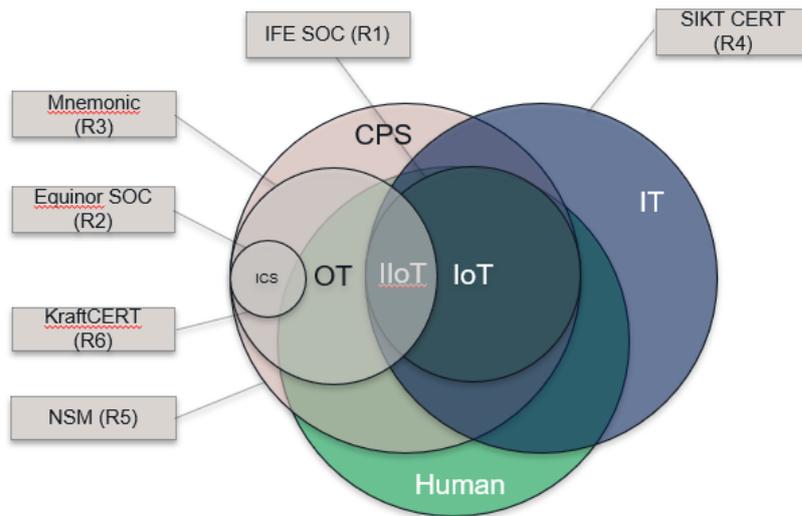


Figure 4.2: The mapping of SOC's system focus in relation to the VENN-diagram

some extent also Operation Technology (OT) devices. With IoT devices, we mean the category of business-oriented devices. Devices falling under the category of IIoT has an industrial-grade approval or certification and are ready to be put into rugged environments. The IIoT device often has the same capabilities as IoT devices regarding connectivity and protocol support, but has additional industrial protocol support like OPC-UA¹, Modbus² or Profibus³ to mention some. OT devices, like PLCs on the other hand, were built for industrial purposes and consist of high-quality components for longer and more reliable operation to use in both critical and non-critical industrial environments. OT devices have often fewer capabilities and must prioritise processing capacity for signal processing from the field devices like a sensor or an actuator. However, the different device types can be a bit confusing in their domain of usage depending on whether it is from OT-, IIoT- or IT domain, but from a device view, and the perspective of a SOC these devices were subject to be part of a security monitoring solution.

4.2 Business drivers

In the business drivers category, we have four themes; "challenges", "background information", "assets" and "threats and vulnerabilities". These themes are mapped to IQ1, IQ2 and IQ3 respectively. In Table 4.2 we provide the result from the analysis with a number of statements with answers matching each theme.

The themes "background" and "assets" have high score and validity for IQ1 and IQ2, while "threats and vulnerabilities" have high validity for IQ2 and IQ3. For the other relevant themes and IQs, the validity was medium to low.

¹Open Platform Communications United Architecture

²<https://modbus.org/>

³<https://www.profibus.com/>

Table 4.2: Analysis of "business drivers" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.

		Business drivers		
RQ	Theme	IQ1	IQ2	IQ3
RQ1	Challenges	7	2	10
RQ2	Metrics, events and alarms	2	6	0
	IT and OT infrastructures	7	11	1
	Devices	2	3	2
RQ3	Human and organizational factors	1	3	0
	Background information	12	13	4
	Assets	5	10	2
	Threats and vulnerabilities	0	8	7
Number of answers with theme mapping		17	31	23

4.2.1 IQ1

In the first interview question, "To what extent would you say that businesses(s) use or have IoT devices?", all the respondents provided answers in the context of business operation with SOC and IoT. The respondents have provided valid answers to describe the use of IoT in their business. For IQ1, we have found valid answers for the themes "background information", "assets" and "threats and vulnerabilities". The IQ1 is linked to RQ3, where we seek historical background information and values through assets in business models for the incentive to support SOC's operational focus towards aligning with security monitoring of IoT devices.

From the mapping of the theme "background information" we found answers with statements for the use of IoT devices in their businesses. In the sector of research and education, the awareness about IoT was low in respect of any knowledge about IoT devices for their customers. This statement is shared by SIKT eduCSC as their focus is mainly towards the IT domain providing infrastructure services to the sector. However, according to SIKT "they probably exist locally" (R4). According to IFE SOC their IoT focus seems to be in the starting position as they state "it is not very common, but we have quite a few units and they are increasing at a rapid rate" (R1). The Norwegian National Security Authority (NSM) states, that several businesses are evaluating and have IoT demonstration projects in sectors like water and wastewater, monitoring flow in manholes and waterways. But also when it comes to building automation systems for "controlling lights, temperature, measuring sensors and door-locks" (R5). "Building automation systems are important and could be critical if the building is housing a critical function or critical information with high value" (R5). The NSM play a central national role in both the IT- and OT domains focusing on developing resilient infrastructures for the society and having a holistic view of security concerns

with "a cross-sectoral professional and supervisory authority within the protective security services in Norway" (NSM, 2020).

According to Equinor (R2), their operation of business relates mainly to the OT domain, but IoT devices were mentioned to be in use, "whether the Equinor SOC has a relationship with IoT or the OT devices... it's okay, historically it's been a bit weak" (R2). In response to business goals and drivers, they state that "our entire business is based on control systems. Platforms and the land facilities are control systems only..." (R2). The InfraCERT play a central role in optimising and "securing of process control systems for the power industry" (KraftCERT, 2023) and "update our customers about relevant vulnerabilities and threats" (KraftCERT, 2023). InfraCERT states that "the hunger for data drives the business in a way to be more efficient and productive" (R6), and when addressing IoT devices "...there is a higher awareness of this than there has been..." (R6) where "the first impression is that their customers have a better overview and awareness of such devices than before" (R6).

The statements presented for IQ1 represent a variety of the provided answer about the awareness of IoT devices. About the IoT VENN-diagram in Figure 4.2 the statements show that every SOC has a different focus on SOC's operation and awareness of IoT devices, depending on their business goals and focus. All six SOCs have answered that IoT devices are in use either directly or indirectly in their businesses today. However, we did not find statements about IQ1 for the theme "threats and vulnerabilities", according to our theme mapping.

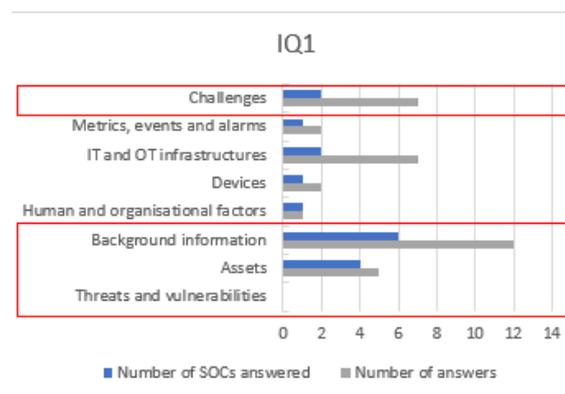


Figure 4.3: Business drivers mapping of themes for IQ1

4.2.2 IQ2

In the second interview question, "How important (critical or dependent) would you say IoT is to your business?", we address the question about business risks of using IoT devices in an existing system landscape. We have mapped IQ2 to RQ3 with the themes "background information", "assets" and "threats and vulnerabilities".

The dependency on IoT devices aligns with the business operation as the known asset to address business continuity and develop emergency response plans to recover from security incidents. However, we have identified several statements and answers with mappings to all three themes, describing the business criticality as a response to the degree of dependency on IoT devices.

Established companies, such as the power industry, have a long history of operating within critical infrastructures. IoT devices are in use in many different areas. IoT devices with sensors

(for measuring capabilities) are often used as add-ons to support or extend the need for more information to make better decisions within their operation.

With the theme "background information" we found insight into the complexity of business operations when addressing the dependability and criticality of systems available in the power industry. According to Equinor, the availability of OT systems is critical when operating complex oil and gas platform infrastructures, a central platform control system "can have up to 200 different subsystems for our largest systems with around 10 different suppliers involved" (R2). Introducing anything new into the existing system landscape will imply a risk for the business. However, NSM made a statement with the use of IoT about critical processes that "no one is there yet... from an IoT perspective - it is too weak and the integrity of such an IoT device is far too low compared to security systems today... but expectations are high within general industrial process control - that it will be extended over time" (R5).

Balancing risks is important and according to Equinor, the design of the underlying OT infrastructures is of high importance when they consider the interface between IT and OT. In these systems, "OT have a more risk-based approach with ISA/IEC-62443⁴ versus IT with typical ISO 27001⁵" (R2) approach. InfraCERT supports national critical infrastructure owners with security competence for IT and OT for "the power industry and partly in oil and gas, which we also cover, they have the requirements to operate in so-called 'Island mode'... so they shouldn't be dependent on it, but the problem became more critical when it comes longer out in the time axis" (R6).

With the responses from SOCs not operating in the critical infrastructures domain, we see the awareness of dependability in IoT devices is less business critical. According to IFE SOC, "it isn't very critical if we lose functionality" (R1), as it may impact some of the ongoing projects and deliveries, but not the whole company to be out of business.

The theme "assets" comes to use when we describe the loss of value with concerns about IoT devices that are in the line of business operation. The consideration of loss implies in reality a negative impact on the business goals and the availability perspective of systems across the entire life cycle. The theme has identified that three out of six SOCs, operating in the OT domain, are more concerned about system outages that potentially could impact business continuity and system availability. Equinor, states that "Within OT, everything from gas control to the safety systems is OT systems that are normally connected to the network. So without the OT systems, the whole company stops!" (R2).

Threats and vulnerabilities are important factors to consider in business operations. We know from IT that regular security updates are crucial to reducing the attack surface for an incident to occur. However, there are some differences between the operational characteristics of the underlying IT and OT infrastructures supporting devices with sensors and actuators. Many of the systems that are in use today, in the OT domain, have often no security measures implemented and have not been part of the security design from the beginning. According to the security provider, Mnemonic, OT systems lacks security measure as "many of these systems does not have any security" (R3). The case is often related to introducing risks of uncertainty in OT networks, where we are "not sure if this could affect the process... it's risky to put things in there that somehow haven't been there before and could affect the process..." (R3). However, when using IoT devices for sensor monitoring in critical processes, NSM implies that IoT "can be critical if they are connected on a critical CPS today... in relation to reporting valve open or whether the pump is running... optimal in relation to the pump curve" (R5). Based on the different answers to IQ2, we found distinct factors of difference between IT- and OT systems, when it comes to criticality and availability, and how the

⁴<https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>

⁵<https://www.iso.org/standard/27001>

different SOC handle risks in their business. IoT devices and systems are identified as important assets in the system landscape today.

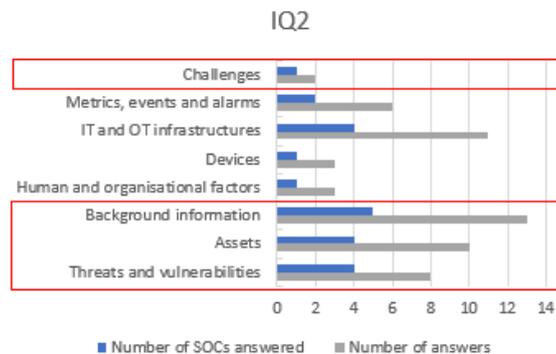


Figure 4.4: Business drivers mapping of themes for IQ2

4.2.3 IQ3

The interview question, "How do you think IoT has or will impact your corporate or enterprise network?", we seek information on how existing infrastructures and networks are impacted when introducing IoT devices. We have linked IQ3 with the themes "challenges", "background information", "assets" and "threats and vulnerabilities". However, during the interviews there was one exception, the IQ3 was left out by a mistake during the interview with Equinor (R2), and therefore the IQ3 were not answered by this participant.

Through the theme "challenges", we found statements describing the negative impact on corporate networks. There is a lack of IoT security monitoring capabilities, we found statements about practices and techniques when introducing IoT devices. According to Mnemonic, network "segmentation is essential" (R3) as part of the defence-in-depth architecture, and is a common practice to reduce business risks when having many different device types in the same network.

A statement shared by IFE SOC of what they believe was caused by a low maturity level for how companies are handling IoT devices today, "we don't believe there are many companies or businesses that have defined separate infrastructures for IoT devices". This would introduce a higher risk of an actual impact on established business networks. IFE SOC also states that "it's harder to get an overview" (R1) when "different types of devices are mixed" (R1). In such cases, it would be challenging to maintain and manage IoT devices. However, this practice changes dramatically for the OT side with ICS equipment. Mnemonic states that, "you do what you can to protect these networks... there aren't that many mistakes to be made until your admin GUI⁶ is on a server that is not protected well enough..." (R3), "the potential damage and the degree of protection for these networks are exceptionally large" (R3). Nevertheless, IoT devices are valuable assets for the owner, if they were aware of their existence and their dependencies for the business.

"Air-gapped systems that are not reachable from the outside, then this can live in its own world and be fine and dandy... but if you connect it online, many vulnerabilities are introduced and such systems are often not designed to be updated..." (R4)

⁶Graphical User Interface

"The large IoT suppliers in Europe and the serious ones who are the 5-6 largest within OT take this seriously - they know that cybersecurity is an enabler to be on the market and this also applies to the IoT devices that these suppliers also sell." (R5)

When considering the statements from "threats and vulnerabilities", the corporate network is an important asset for every business and should have protective measures for handling threats introduced by IoT devices. According to Mnemonic, the corporate network is "the most important asset to protect" (R3). Threat actors are "looking for a foothold... if these actors find a system that is reachable from the internet, they will do anything to get in..." (R3). The assumptions of higher maturity level and awareness of IoT in the business depends on, if "the businesses are part of a security model - i.e. it is intended that they should be part of an existing security model, they will probably be safe and secure" (R5).

Introducing IoT devices in existing infrastructure without having enough information about their functionality and possible vulnerabilities would implicitly have a negative impact on the corporate network. According to NSM, "that it is in addition to - then you have to plug yourself in on the outside... then it will affect both the company and the business network negatively in that it constitutes an attack surface and vulnerabilities" (R5). The attack surface for a corporate network was further challenged if non-existing management and maintenance processes of IoT devices are in place. However, InfraCERT states that the awareness about IoT is rising, where they "actually see that it affects the business network in a positive direction... because now you have to look at the security around this..." (SCO6).

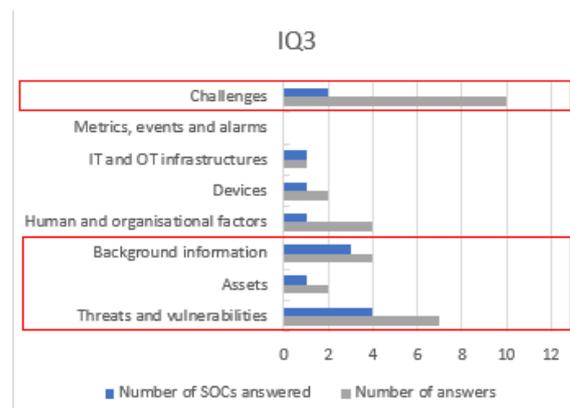


Figure 4.5: Business drivers mapping of themes for IQ3

4.3 IoT management

Managing IoT devices can be a complex task without established operational processes, tools and technologies for life cycle management. Proper management tools to cover onboarding and provisioning of devices, configuration, upgrading and end-of-life through off-boarding of devices were identified as a need. We will through the category IoT management present the results from the IQ4, IQ5 and IQ6 using the themes "challenges", "metrics, events and alarms", "IT and IT infrastructures" and "devices".

The themes "challenges" have a high score and validity for IQ5 while "IT and OT infrastructures" have a high validity for IQ4 and IQ6. The theme "devices" have a high validity for IQ6 and for the other relevant themes and IQs, the validity was medium to low.

In Table 4.3 we present an overview of the number of statements and answers with the corresponding theme mappings.

Table 4.3: Analysis of "IoT management" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOC's provided an answer and the corresponding theme mapping.

		IoT management		
RQ	Theme	IQ4	IQ5	IQ6
RQ1	Challenges	2	45	7
RQ2	Metrics, events and alarms	12	0	14
	IT and OT infrastructures	14	2	34
	Devices	3	0	4
RQ3	Human and organizational factors	0	0	1
	Background information	9	2	1
	Assets	0	0	1
	Threats and vulnerabilities	0	5	3
Number of answers with theme mapping		29	45	52

4.3.1 IQ4

With IQ4, "Do you distinguish between IoT, Industry-IoT and Operational Technology (OT) devices in how you handle and operate these devices/systems?", we have mapped the question to the themes "IT and OT infrastructures", "devices" and "metrics, events and alarm". The "IT and OT infrastructure" theme describes the underlying infrastructure and architecture layers, for example, where to put the different devices.

According to IFE SOC, "you usually want to segment OT from IoT" (R1) and suggest to "segment the network based on the availability perspective of the system and what is critical and not critical..." (R1) and group devices, "which communicate with each other... and place those which are critical to operating mostly for themselves..." (R1). The use of the ISA/IEC-62443⁷ standard as the cybersecurity framework for OT environments and ICS networks has been mentioned by the SOC's, working especially within industrial process control systems.

Device separation and network segmentation are said to be the technique used to group devices with the same functionality together. Traditionally the OT networks were often designed as flat Layer2⁸ networks, connecting series of field devices with sensors and actuators. Nowadays, with the emerging threat landscape towards OT, InfraCERT has mentioned that "you have to start with segmentation out in the process networks..." (R6), it is not enough to rely on the defence-in-depth design approach from the perspective of IT. In the context of management of IoT devices,

⁷<https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>

⁸<https://www.firewall.cx/networking-topics/the-osi-model/173-osi-layer2.html>

Equinor has mentioned that it is "not very much handling or extensive use of industrial IoT" (R2) in their business operation.

The practice within IoT, Industry-IoT and OT in how we handle different devices in today's system landscape, where operations are partly adopted from a defence-in-depth approach and the ISA/IEC-62443 standard. According to NSM, "the SME⁹ market, don't have the ability to implement it as a whole or to follow that process fully and throughout the lifetime of the systems - it quickly becomes piecemeal and divided" (R5). However, implementing and following these types of standards to their full extent would be costly for the extension of the infrastructure with several new network zones and conduits for controlling the network traffic. In addition, the demand for available competencies within IT/OT and operational personnel are rising (Vavra, 2021). The cost-benefit model exists in every business, and in this context, it is about balancing the double-edged sword to fit the business model.

In the theme "devices" we have identified some types of devices within IoT and Industry-IoT. IoT devices are often cheaper in procurement than OT equipment, and NSM mentions that "it will probably merge over time... but for now, OT is like an umbrella on top - where you increase with different connectivity in the form of IoT..." (R5). IoT devices are instruments that could be placed temporally inside different networks for measurements or extending functionality. According to NSM, "areas of use can be a battery-powered vibration sensor e.g. where you have a compressor that you suspect has some problems with a bearing for example, then you can connect cheap battery sensors that you can connect to a random network to get an indication of the state of the machine, but you would never connect something like that into a DCS system (distributed control system) to do management" (R5).

On a high-level view, there is more focus on the network infrastructures as the security perimeter for where to place devices and less on the security measures for the actual device itself based on the themes mapping, from the answers given to IQ4. However, health monitoring of IoT devices which we would map to the theme "metrics, events and alarm", was mentioned by Mnemonic to be something that we should give more attention to when handling IoT devices. According to Mnemonic, "you must ensure health monitoring as well and ensure that there is actually traffic we see there" (R3) on the network. Based on the different SOC's answers above, there was a distinction between OT including IIoT and IT including IoT, in how such devices are handled.

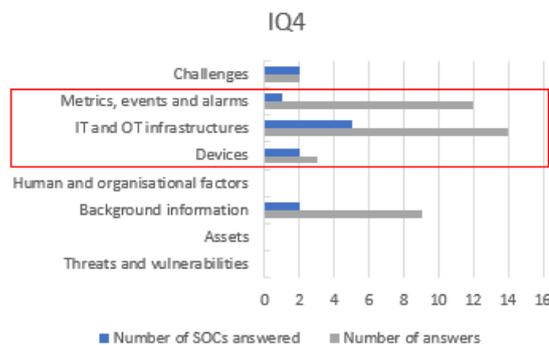


Figure 4.6: IoT Management mapping of themes for IQ4

⁹Small Medium Enterprises

4.3.2 IQ5

With the IQ5, "What would you say are the challenges with different IoT systems today?", the SOCs shared many of their experiences and challenges from an operational perspective. We have mapped IQ5 with the theme "challenges" to identify problems to overcome that would prevent efficient management of IoT systems.

The following statements were mentioned to describe some of these challenges, "For a SOC, it is challenging to keep track of everything..." (R1) and "if you have many systems, there are always some systems that are not up to date..." (R1) which introduces an attack surface with a gap between different systems vulnerabilities and possible exploitation. These two statements are shared by IFE SOC and explain the challenges of maintaining an up-to-date fleet of devices and systems. The fact that this was a time-consuming task to complete, and it would require product-specific competencies that potentially only would be available by the different suppliers or vendors. The complexity is rising, when we introduce many different systems in operation. From the SOC's operational perspective, the following challenges are mentioned:

"The biggest challenges - discovering abnormal things that are happening..." (R2)

"You do not have expertise in all the systems, so you are very dependent on the suppliers!" (R2)

"The more such systems you put into a monitoring solution, the larger that matrix becomes." (R3)

"...very much of the context around this (systems) requires you to work with this at all times... it is in a way a challenge..." (R3)

"...it is not so easy to streamline the operation of such systems... it is often tailoring and different systems that can be a big challenge... both with expertise and resources..." (R4)

However, this reveals a need for common methods, tools and technical requirements for establishing life cycle management of new and existing IoT devices. According to NSM experiences, there were "IoT devices that have no security in the component structure in relation to OSI¹⁰ layers" (R5), were already in the design phase, and there is a lack of requirements to address the need to "secure the protocol on which IoT devices communicates on..." (R5).

These challenges can partly be explained by the lack of defined processes for adopting new devices throughout the life cycle management, but also what could happen when not addressing technical requirements to achieve adequate fleet management of many different IoT devices at the same time. InfraCERT has experience with different IoT vendors, "...usually on the non-industrial side, it's more like "set-and-forget", they sell them and then they are no longer supported..." (R6). However, this could be explained as a result of poor procurement and implementation processes, when not defining needs and technical requirements for handling IoT devices. The following challenges were technical statements about typical IoT devices, shared by InfraCERT;

"...very few have the possibility of remote updating..." (R6)

"...very few have the possibility to send the logs you actually need..." (R6)

¹⁰Open Systems Interconnection model (OSI model)

"...very few have the option of a host-based firewall..." (R6)

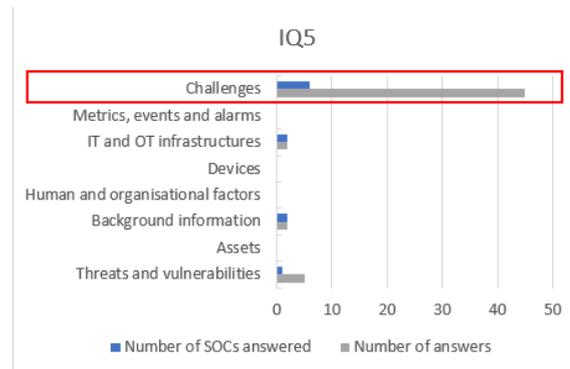


Figure 4.7: IoT Management mapping of themes for IQ5

4.3.3 IQ6

For our last question in the category of IoT management, we asked, "What type of security barriers/mechanisms are necessary to protect such IoT devices?". We have mapped IQ6 with the themes "metrics, events and alarms", "IT and OT infrastructures" and "devices".

The protection of IoT devices can be achieved using different techniques and methods, with layers of security, covering protection mechanisms on the device itself, to protect the communication for availability and reliability on the underlying infrastructure. Starting with the network, to which the IoT device is connected to, we will use the theme "IT and OT infrastructure" to describe technical aspects of security protection barriers.

According to Equinor, "the perimeter defence thing has a bad reputation... it's a bit old-fashioned, but it's absolutely necessary" (R2) to successfully protect critical devices from unwanted traffic that could influence the operation. The defensive approach is based on the ISO/IEC 62443 network zone model, where we limit the device's ability to communicate between network segments using conduits or firewalls to block unwanted network traffic and control access to specific services. Endpoint detection and response (EDR), are tools used on devices for detecting anomalies and mitigating with a response to recover from a security incident. However, this was something that would require a full operating system and is more common on computers acting as engineering workstations for the management of PLCs. The ISO/IEC 62443 standard is based on the Purdue model from 1989 (Mathezer, 2021), which is working as the reference network architecture model on how to configure and secure industrial control system networks. The network model introduces principals for traffic flow directions between network segments, defined as zones, from the lowest level 0, where the field devices were connected and communicating in the upwards directions to level 1, comprised by the local device controllers. The next level, level 2, consists of a local supervisor for monitoring and control of devices, towards level 3 for management and alarm handling, before entering level 4 and the business network.

Before entering each level, the access is controlled by different barriers and according to Equinor, the protection mechanism "between level 3.5 and 4 it is two-factor authentication, logging, jump hosts, we build up our jump hosts every other day so that persistence will be almost impossible to achieve..." (R2). This approach adds up to how we design the networks, and according to NSM, "the security barriers that are implemented, mostly rely on having good networks - the backbone is the most critical thing" (R5). Another security mechanism mentioned by Equinor, is

the use of EDR tools for detecting anomalies, when entering "at level 3 we are in a disconnected state from the networks where there is real-time traffic, so there we are a big fan of using EDR tools such as Defender" (R2). Defender¹¹ is the name of Microsoft's endpoint protection product to defend against malicious cyber threats. Mnemonic mentioned that "the way to go is to build as many layers of security around as possible..." (R3). The SOCs have provided several statements addressing security mechanisms that would be beneficial to consider when protecting IoT devices:

"...log analysis will be... and is an increasingly important detection mechanism for us..." (R3)

"metrics and optics, the heart-beat protocol did that and reported on versions, battery life, temperature, humidity etc... in addition to sending properties back to the system" (R5)

"segment down to the minimum function and have the traffic gathered at a central point for control..." (R6)

"...possibilities for host firewall, whitelisting of traffic on the device itself..." (R6)

"authentication mechanisms... central authentication mechanisms... are of course a very important part of this because without this you will e.g. end up with the same password on all devices..." (R6)

In addition, in regards to operating system hardening, we would instead of using third-party tools as addons for management, prefer to use 'Living Off the Land Binaries' (LOLBins). LOLBins are tools that are available through the operating system and already exist on the device. This would allow us to follow the existing update regime from the given operating system vendor when applying security patches. Equinor has mentioned, "use the machine's own tools to produce things.. typical scripts and batch commands..." (R2). However, this would be a beneficial principle to follow for any device, by starting to use existing tools to harden the operating system and turning off features that are not in use.

Through the theme "metrics, events and alarms" we have gained insights into what type of information would be useful for a SOC to know about when protecting IoT devices and what is essential:

"...important to know who communicated with the PLC..." (R2)

"...which commands are sent..." (R2)

"...good overview of the IoT devices that are in your network..." (R5)

"...how they behave in your network..." (R5)

"...run measurements on the IoT devices you have, all the way down to MAC level and IP addresses – data flow, netflow etc. – run thresholds on bits and bytes to see what is normal communication..." (R5)

"...monitoring traffic, which I would say is equally important as the log sources...to see movements in the network..." (R6)

¹¹<https://www.microsoft.com/en-us/security/business/microsoft-defender>

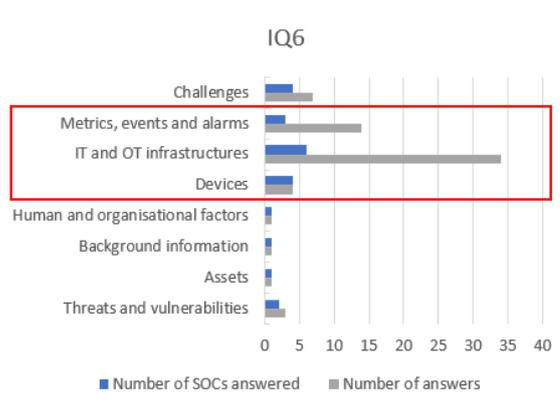


Figure 4.8: IoT Management mapping of themes for IQ6

4.4 Monitoring and detection

From a SOC perspective, the ability to detect abnormal activities in the infrastructure is crucial for handling and mitigating security incidents. Before an event or alarm turns into an incident for a SOC to manage, there are several processing steps to be performed from logs sources. The need for log information from network equipment, i.e. switches, firewalls, intrusion detection systems (IDS) and endpoints are important sources for analysis and development of detection capabilities. However, we have identified from the literature, a lack of monitoring capabilities when it comes to IoT devices. Therefore, the current practices are often relying on network information and the investigation of network traffic for detecting anomalies. With relevant parameters from the IoT device, we are able to make detection mechanisms based on system events. Using log events from different sources we have the possibility of correlating and finding the logic in a series of events to trigger alarms for attention and further investigations. To help us understand and distinguish between an event, alarm and incident, Daniel Miessler¹², has analysed several different definitions of these terms from the industry and came up with three describing definitions (Miessler, 2021): (1) "An event is an observed change to the normal behaviour of a system, environment, process, workflow or person", (2) "An alert is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action." and (3) "An incident is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business."

To achieve proactively monitoring, logs from several sources were required, including end-to-end traffic monitoring and parameters from IoT devices. A fully-fledged operating system would provide us with richer event information that benefits better detection quality. When using the same approach to address IoT monitoring, there is a gap in available logs provided by the different IoT devices and vendors for efficient detection. IoT devices have limited resources to do additional tasks like extensive logging with security in mind. We will through the category monitoring and detection present the answers to IQ7, IQ8 and IQ9 using the mappings of the themes "challenges", "metrics, events and alarms", "IT and OT infrastructure", "devices" and "human and organisational factors" presented in Table 4.4.

¹²<https://danielmiessler.com/>

The themes "metrics, events and alarms" have a high score and validity for IQ7 and IQ8, while "IT and OT infrastructures" have a high validity for IQ7, IQ8 and IQ9. For the other relevant themes and IQs, the validity was scored as a medium.

Table 4.4: Analysis of "monitoring and detection" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.

RQ	Theme	Monitoring and detection		
		IQ7	IQ8	IQ9
RQ1	Challenges		20	0
RQ2	Metrics, events and alarms			
	IT and OT infrastructures			
	Devices			
RQ3	Human and organizational factors		0	0
	Background information	2	2	0
	Assets	0	0	0
	Threats and vulnerabilities	13	0	0
Number of answers with theme mapping		40	42	11

4.4.1 IQ7

With IQ7, "How should IoT devices be maintained and monitored?", we seek information about current best practices and new approaches for managing and monitoring devices. The IQ7 is mapped to the themes "challenges", "metrics, events and alarms", "IT and OT infrastructures" and "devices". We have valid scores when considering the number of SOCs that have provided an answer and the number of answers for all themes.

With the theme "challenges" three of six SOCs have answered, and we are addressing IoT device monitoring issues describing lack of security measures, health parameters and log capabilities from devices with low resources. There is a wide spectre of devices and different capabilities when considering the monitoring subject. In general and according to IFE SOC, there is "too little information to monitor on..." (R1), and "the problem is probably getting some good data out of the devices..." (R1). It is time-consuming to reverse engineer devices to find possible parameters to include in monitoring and detection scenarios, this is often the case when dealing with the closed ecosystem and vendor lock-in solutions, and requires both closer communication and interaction with the vendors.

"The problem is partly that it is proprietary, and then there is not so much focus on getting out the parameters you need to be able to monitor..." (R1)

"encryption will only harm the possibility of detection, as we lose insight into what is happening on the network and the attacker..." (R2)

Depending on the implemented solution and setup of a management system for OT devices, the use of authentication is a security mechanism that would benefit the verification of who is doing what and when on a PLC. A statement shared by Equinor implies its relevance, "...at level 1 between the PLCs, authentication is very important..." (R2).

With the maintenance of IoT devices, we address the identification of capabilities for how to typically update devices with firmware and security patches, maintaining and changing the configuration. The degree of automation for patch management would depend on the criticality and availability factors for how long downtime of a device would be tolerated.

"patch management or vulnerability management that you have on other devices... you have to do a regular round to check if things are updated... check if there are patches if it's not automatic..." (R6)

"we simply do not have the capacity or maturity to look at vulnerability management quite yet..." (R2)

The theme "IT and OT infrastructures" provided information about components and tools that were used in monitoring devices in an infrastructure. The SOC at Equinor have shared some experience about tools for scanning for vulnerabilities, "...on the SOC side, we have vulnerability management which scans the enterprise network both from the inside and the outside..." (R2), as one example of vulnerability scanning of OT networks, the use of "Tenable, which makes the Nessus vulnerability scanning software, has an OT module" (R2). Tenable¹³ is a vulnerability scanner platform targeting IT infrastructures. However, when dealing with OT networks, tools are not available. According to Equinor, they are using customised tools provided by the engineering workstation when "patching of PLCs, I have created a solution that is installed on everything from level 2 upwards in the pardue (ISA/IEC-62443) model that gives status on all Windows machines and patch level...". The availability of security updates is an important factor for maintaining a stable and up-to-date infrastructure environment when considering the life cycle of devices. NSM has mentioned the importance of "...have a vulnerability software update for devices, there should be a minimum requirement that the supplier provides life cycle vulnerability updates for the product you buy..." (R5). The Common Vulnerability Scoring System (CVSS) is an established method maintained by the Forum of Incident Response and Security Teams (FIRST) for capturing characteristics of vulnerabilities and producing a numerical scoring system to reflect severity (FIRST, 2023). However, the CVSS does not measure or quantify the risk and would require more knowledge about the infrastructure and where the device is located. Equinor has mentioned that tools like "Dragos e.g. has done a lot of good work to assess the CVSS score on the vulnerabilities and map it against the actual risk..." (R2) for the IT and OT infrastructures. Dragos¹⁴ is a cybersecurity platform for protecting OT and industrial systems.

With the theme "metrics, events and alarms" we have gathered valid answers from five of six SOCs for IQ7. This theme represents, types of monitoring parameters the SOCs would find useful and available from different IoT infrastructure components. Statements include:

"The gateways are probably not that bad compared to what you can get out of the monitoring parameters..." (R1)

¹³<https://www.tenable.com/>

¹⁴<https://www.dragos.com/>

"Know who is logged on your Windows machine..." (R2)

"...which commands are sent..." (R2)

"What can you get of information by listening on the network, and then there is less risk of affecting the PLC as well..." (R2)

"Need insight into the communication between that machine and the PLC..." (R2)

"...insight into the PLC's switch if there are other IPs that talked to the PLC..." (R2)

"A good overview of the IoT devices that are in your network..." (R5)

"...you have to have logs to know what's going on... without logs, you're blind..." (R4)

"alarm fatigue is very real there are so many alarms..." (R6)

"...health monitoring and monitoring and follow-up of this... at any time... and then you have to try to build as much detection around as possible..." (R3)

The theme "devices" have statements for IQ7 representing how IoT devices are used and put into action in an infrastructure. InfraCERT has shared that device fleet management using configuration profiles are important capability for handling many devices, "this with profiles is important so that you can tune many devices at the same time..." (R6). However, the opposite of doing active device management, is to do nothing about the device after it is "configured a certain way and then left without further attention" or management, and remains connected to the infrastructure. This is called a 'set-and-forget' practice and would introduce an increase in risks depending on the type of use case and where the device is connected. NSM has shared an example of such usage for IoT devices in "...hydropower and rural areas, power producers and power distributors, then there is probably a bit more of 'set and forget' usage - that these devices are deployed to do a simple job - where the devices send data in and no more maintenance than that..." (R5). According to Mnemonic, "...there are pros and cons - it's the most critical systems you have that you have to protect and it may not be these systems that are the most widespread..." (R3), when it comes to a 'set-and-forget' practice.

For the theme "human and organisational factors" we look at the process interaction level and address the human aspect within the organisational structures as this often implies the managing of risks in infrastructures. The need for introducing changes in a system landscape in production introduces a potential negative influence or impact on devices and underlying networks. Equinor has a statement describing how they work when introducing technical changes by always considering "what risk do I take away if I do something, and what risk do I add by doing it..." (R2). This implies a strong need for competence and knowledge about the type of device and its possible impact on other systems. According to InfraCERT's experiences, that it is, "...very individual-based on who is involved in setting up the solution and who makes requirements when you buy such a system..." (R6). The interaction and communication between all parties when introducing changes to devices and infrastructure are mentioned to be a success factor, however, InfraCERT has stated that:

"...those who buy a SOC service where the SOC has many customers, it is very difficult to understand how things move in the network..." (R6)

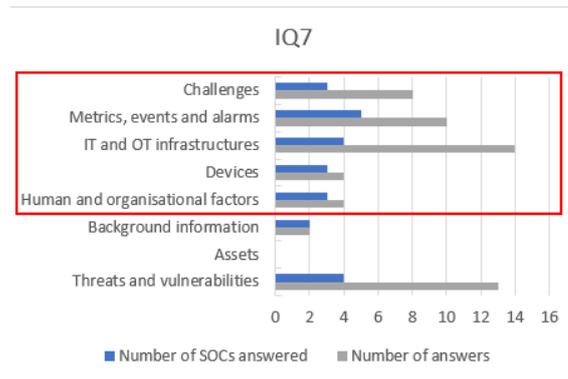


Figure 4.9: Monitoring and detection of themes for IQ7

4.4.2 IQ8

With IQ8, we ask, "How do IoT devices log and report?". We mapped the question to the themes "devices", "IT and OT infrastructures" and "metrics, events and alarms". For theme "devices", we don't have any statement mapped for IQ8 using this method. However, for the theme "metrics, events and alarms" we have valid answers from five out of six SOCs, and 31 statements describing the type of information a SOC would need from devices, the operating system and the underlying network infrastructures. We shared the twelve most relevant devices and network security statements that were mentioned to be beneficial for SOC's detection capabilities below:

"...breach of network protocol..." (R1)

"typical counters for packets that are not valid..." (R1)

...we have a solution that retrieves both maintenance information such as CPU, memory, disk space and a little more security information.. (R2)

"When was the last time the password was changed?" (R2)

"Which USB IDs exist?" (R2)

"Which wireless networks are used?" (R2)

"What I miss the most, is the insight into traffic between the PLC and engineering workstation... is anyone changing the security logic?!" (R2)

"The heartbeat and netflow are essential!" (R5)

"Type of heartbeat and validity check that the device you plug in last year is the same this year... e.g. kind of mac locking in a way..." (R5)

"Could bring a minimum of a schema from a data model for what is to be sent from an IoT device..." (R5)

"What type of function it has...?" (R6)

"...know what patch level it has..." (R6)

According to NSM, logging capabilities are essential and should be supported by a central logging infrastructure for secure storage preservation and for searching the logs, in case of a security incident, "It is important that you send all logs to a central log server, and use that log server in the event of an incident..." (R5). All logs and meta information gathered at the same time, would be a valuable asset for further enrichment and "link this to the vulnerability database to know what to look for..." (R6).

The theme "IT and OT infrastructures" provides more information about what types of logging systems are in use in different organisations. Equinor has shared the type of tools used, Splunk¹⁵ when dealing with device logs for asset inventory, "We use Splunk as an inventory tool and not as a SIEM" (R2). Splunk is a software-based platform leveraging capabilities for collecting, searching, analysing and visualising log data. Logs are multipurpose sources of information and can tell a story about what is happening in your infrastructure, if "...your devices are wiped and that the memory and disk are wiped where the IoT device is located, and if you do not have a central log server that can capture this over time, you are left with very little if you are going to run forensics..." (R5)

Having device logs available and in active use would change the way we detect any changes in the network by utilising real-time log queries for detection in air-gapped systems, "which can be used for threat-hunting and that is because we cannot give the production control systems access to our main system" (R2). For IoT devices in particular we are facing a more open architecture and network protocols. A statement mentioned by NSM says that "the lion's share in the IoT world is on the other side of the scale - i.e. they are not proprietary and can run normal IP, WiFi, Bluetooth protocols that everyone can read..." (R5).

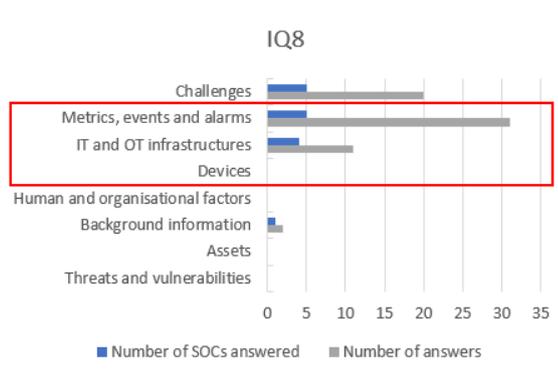


Figure 4.10: Monitoring and detection mapping of themes for IQ8

4.4.3 IQ9

For the IQ9, "Is edge computing or central gateway for monitoring IoT devices something that is used today?", we investigated if there are practical use cases or information about the planned use of a new technology utilising edge computing for monitoring, which is closely connected to the IoT device in the edge of the network. The IQ9 is mapped to the themes "metric, events and alarms", "IT and OT infrastructure" and "devices". We have collected eleven valid statements from four of the six SOCs for the theme "IT and OT infrastructure", which were the only theme with answers for IQ9.

The edge computing concept was mentioned by Mnemonic for detection closer to the devices, "call it distributed detection, then you can build the detection in another way perhaps... by building logic closer to the sensor... and chewing everything through the same engine..." (R3) on

¹⁵<https://www.splunk.com>

the edge of the network. Zero trust is mentioned by NSM, as a new movement and architecture design in enterprises towards, "the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources" (Rose et al., 2020). NIST has defined Zero Trust (ZT) as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised." (Rose et al., 2020, p. 4). Much like the opposite of the defence-in-depth architecture we earlier have presented. In the context of edge computing the use of Zero trust is a new approach and according to NSM such a journey would start by "...divide the elephant into smaller portions, I would say it is possible to think zero-trust and aim to run it out on the edge part..." (R5). This is, however, challenging and would require a complete redesign of current infrastructures and network services, according to NSM, this would "...not be holistically on established infrastructures - it doesn't work... it's far too expensive and in addition, you have devices that cannot be converted to run towards a Zero-trust mindset..." (R5). The use of cloud services where edge computing is a part of the local infrastructure is mentioned by Equinor, "we have started to get some systems, as ABB calls it, edge gateways that take process values and send them up to a cloud for processing and optimisation, where we currently have no monitoring..." (R2). The following statements were also mentioned in combination with edge computing technologies:

"It is challenging to turn around when you have established practices..." (R5)

"...very many (organisations) have central monitoring..." (R6)

"...you must have a full top rig with the next-generation firewall..." (R6)

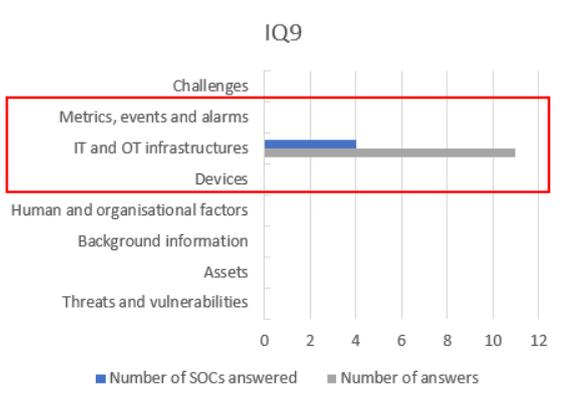


Figure 4.11: Monitoring and detection mapping of themes for IQ9

4.5 Security Operation Centre (SOC)

One of the SOC's main purposes is to provide situational awareness for the organisation regarding security-related activities. Identifying these activities requires insight and knowledge through the use of filtering and applying logic's using patterns on many different log sources. A SOC is instrumented to provide a "real-time view into a network or an organization's security status" (Nathans, 2014, p. 3). How would this situation awareness look like from a SOC perspective in

relation to IoT- devices and systems? We present the answers from the SOC category for IQ10, IQ11, IQ12 and IQ13 using the mapped theme "human and organisational factors". In addition, we have mapped the IQ11 to the theme "challenges" and RQ1, with statements describing the perspective of a SOC through organisational challenges. For the theme "human and organisational factors", we collected and mapped 57 statements with RQ3 from all six SOCs, presented in Table 4.6.

The themes "human and organisational factors" have a high score and validity for IQ10, IQ11, IQ12 and IQ13, while the theme "challenges" had a medium score of validity for IQ11.

Table 4.5: Analysis of "SOC" in relation to themes and statements (answers). The table shows the results from theme mappings using the validity scoring system. The statements were grouped by the number of SOCs provided an answer and the corresponding theme mapping.

		SOC			
RQ	Theme	IQ10	IQ11	IQ12	IQ13
RQ1	Challenges	5	7	3	2
RQ2	Metrics, events and alarms	7	0	0	1
	IT and OT infrastructures	2	4	0	4
	Devices	4	1	0	0
RQ3	Human and organizational factors	21	13	11	12
	Background information	0	0	0	0
	Assets	0	0	0	0
	Threats and vulnerabilities	1	0	1	0
Number of answers with theme mapping		21	20	11	12

4.5.1 IQ10

For the IQ10, "How do you think IoT devices should be introduced to a SOC team for security monitoring?", we asked the SOCs how security monitoring of IoT devices should be introduced to the team. The IQ10 were mapped to the theme "human and organisational factors" and points to statements that address awareness, competency and complexity. When introducing IoT devices for a SOC team, the degree of awareness of IoT devices and the business objectives for using IoT was essential. There could be aspects from legacy systems with proprietary protocols (ethernet and wifi) and organisational procurement processes which prevent the SOC's ability to consider proper security measures of IoT systems.

However, awareness is about knowing and understanding what is going on in the network and the organisation. A statement shared by NSM addresses the absence of IoT awareness within, "established security teams do not have a good relationship with IoT devices..." (R5). So what could this depend on in an organisation and within SOC teams?, "...it is for some a cultural journey..." (R5), with such a statement, we considered this with a low score for the organisational maturity level of adoption and uptake of new technology and even the opposite effect to replace legacy technologies and systems.

IFE SOC has mentioned that "generally I believe that IoT devices are not so much of focus in SOC teams - they are more seen as network devices..." (R1), and InfraCERT have mentioned that IoT devices should be considered more seriously, when being introduced to existing network infrastructure, meeting possible new requirements, so "the question becomes more about being able to place them into a system..." (R6). Short-cutting defined implementation processes, when onboarding new devices would potentially introduce new risks into the existing system landscape, when placing devices into the wrong network zones without protection and monitoring options.

These types of situations were mentioned by NSM, as possible consequences when "a migration of risk involving IoT can potentially migrate to legacy systems that do not have a good self-protection and security model thinking..." (R5). The modus operandi for organisations and SOC teams introducing new devices in the systems landscape could be to consider a zero-trust model for IoT devices. NSM has shared two statements that would support this approach:

"Don't trust devices until you have good control over the network from inside and where the device sends data..." (R5)

"Important to have zero trust in these IoT devices from day one!" (R5)

The complexity of the incident handling involving IoT devices would require emergency preparedness skills and the possible need of involving other parts of the organisation and external parties, including the suppliers. Equinor has mentioned they are, "...quite dependent on suppliers if something happens..." (R2) regarding OT systems. However, in comparison "handling a case from IT... you typically can manage 50 cases a day if they are simple, but when it comes to an OT case, a case can take days..." (R2).

Complexity matters, when the workload for a SOC were rising and to withstand managing and handling incidents over time. This requires the consumption of both personnel and the right skills and competency. In general, with such a statement we would assume the need for recruiting personnel and building competencies to make the gap smaller when introducing IoT devices. Equinor has mentioned they have good experiences with actively recruiting experienced personnel from the OT domain, "we are recruiting people from OT environments... it's not just informatics people... there are people who have some background from OT so they know what it's all about..." (R2).

Security monitoring of IoT devices is somewhat a new field of expertise, and according to Mnemonic, "in one way, you have to build competence stone by stone when it comes to expertise, and here you need that type of asset information to build expertise around this..." (R3).

"that the SOC does not have very much knowledge about what is outside classic ethernet networks... nor what takes place in the traffic itself..." (R1)

"after all, there are only a few in these companies, who dares to almost log into such GUIs... for fear of destroying it..." (R3)

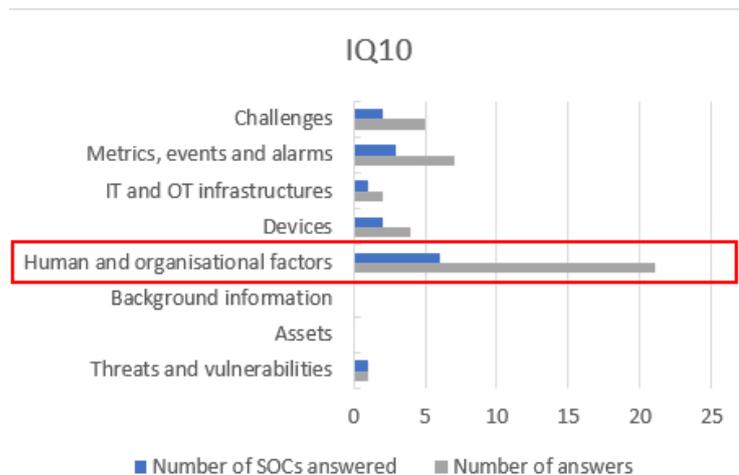


Figure 4.12: Security Operation Centre mapping of themes for IQ10

4.5.2 IQ11

The IQ11, "How do you think SOC should be organised for optimal monitoring of IoT devices?", is a question more directed to finding the participant's reflection on how to organise a SOC in such situations. We searched for their opinions from the perspective of establishing security teams for how this could be done when introducing IoT devices for security monitoring. The IQ11 were mapped to the theme "challenges", where we collected fewer statements from only two of six SOC. The theme "human and organisational factors" have, however, a high number of statements mapped and answered by all six SOC.

Equinor has shared a statement that describes how they organise the SOC, utilising different specialist groups, "we have one SOC, and such subject matter experts as we call them... some must be good at cloud, some at OT..." (R2).

A SOC can be best recognised as a team-based organisation, where each team are organised into different competence or specialist group, based on their skills and knowledge of systems to support. However, when addressing the theme of "challenges" we quickly met the competence gap when evaluating the mapped statements; finding an optimal organisation regime for monitoring IoT devices. According to IFE SOC, there were "two worlds that meet in a way - traditional SOC has focused on software and devices - and in a way things that run and communicates - not so much on management and other types of protocols..." (R1), another statement described that IoT competence can be hard to find and should be built from the inside of an organisation, "I believe that most SOC organisations will have problems with handling IoT devices knowledge wise..." (R1).

The strength of organisational affiliation should not be underestimated when building new domain knowledge. According to NSM, IoT devices should be introduced using a process-based approach applying a "plan, implement, operate and improve - getting it into the normal cycle of the SOC..." (R5). However, the overarching process for improvement was described by Equinor as the challenge of getting hold of logs and information from the assets, "most of my time or 80% of my working day is not about detection, but getting enough data in..." (R2). A consequence of having enough logs would be to improve the detection capabilities by generating more reliable alarms that can be directed to specialised teams. Time is crucial when handling incidents, and instead of sending alarms to a generic alarm queue for SOC personnel to handle, it would be quicker to find a mitigating action by sending tailored alarms directly to a team. Equinor shared a statement about

regular alarm queues and was experiencing that, "a SOC should be a common organisation and be disconnected from regular alarm queues, they do not need to have the same alarm queue..." (R2)

"the preventive part... it will probably quickly be handled by more specialised people..."
(R1)

Organising SOCs into more specialised teams was found to be a common approach in some of the SOCs depending on size. Mnemonic, which provides SOC services for a broad range of companies and different types of businesses, was using teams grouped by competencies and department affiliation. They have many security analysts covering log analysis and detection capabilities for their customers. Internally, they have organised into different departments based on what the team were working on. They have dedicated people working with OT systems, network infrastructures, and log analysis. Mnemonic mentions how they were organising personnel for security monitoring in the following statement, "...we use these analysts because they want to analyse these alarms first regardless... whether they come from an OT network or not... and of course, they have escalation links where possible... when things have to be investigated further..." (R3).

When working on improving security monitoring, the interaction with complementary competencies in each team is key to developing better detection mechanisms. A closer interaction with the suppliers when improving the monitoring of devices was mentioned by InfraCERT, to be "...naturally because the expertise is found with the suppliers..." (R6). The lack of expertise was stated as one important factor to address when considering how to plan and organise a SOC for optimal security monitoring.

"...doubt that anyone is as proactive as this – most are probably more reactive..." (R5)

"...believe that those who have this in-house will probably have their own OT team..." (R6)

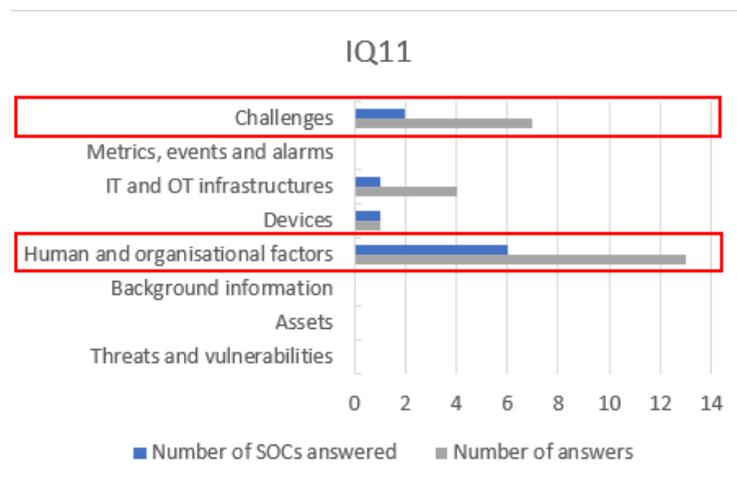


Figure 4.13: Security Operation Centre mapping of themes for IQ11

4.5.3 IQ12

With the IQ12, "In what way is the organisation of the SOC influenced by the business objectives?", we seek information about how a SOC would be organised to align with the business objective. We have mapped the theme "human and organisational factors" with IQ12 and RQ3.

The internal organisation of a SOC should reflect what type of operating model was chosen for the business. The possibility to scale an organisation according to the needs and demands from an operational stand is mentioned as an important factor. According to SIKT, "...the more serious incidents, the more management must be sure that there are no security gaps... and more resources must be allocated..." (R4). For an organisation to be able to prioritise, requires capabilities for internal communication and established escalation links with the upper management, but also the acceptance for using time to improve these internal processes. Equinor has shared a statement addressing prioritisation, "if something happens at a facility, they always get first priority, so you always get acceptance to use the time you need to operate the OT systems..." (R2). However, being able to prioritise would require a holistic view of organisational activities and processes. IFE SOC has shared a statement that likely would have a negative impact on the SOC operation capabilities when the organisation were "...procuring solutions without involving the SOC, it is difficult to detect that something new is being introduced..." (R1).

The damaging impact on OT systems is very large if a perpetrator managed to turn components off and change configuration settings. According to Mnemonic, "...so then you depend on having an operations centre or a functioning monitoring solution..." (R3) to protect, develop security measures and monitor critical systems. Whether the core business objectives were aligned with the SOC, would depend on how integrated and dependent the business is on protecting important functions or systems. A SOC should work closely with the organisation and work proactively on reducing the organisational risks. According to NSM, a SOC should focus on the alignment with the business objectives, otherwise, the organisation surrounding, it "can result in getting a business that is down for a longer period of time..." (R5). NSM has also shared some more statements pointing towards the need for organisational awareness addressing risks on IoT systems:

"weekly measurement of how critical those systems are..." (R5)

"highlight that a SOC is important, both for having systems up and running, but also for detecting daily operations and detecting anomalies where it has been set up and acting in relation to the ranking of the alarms..." (R5)

Organising a SOC would depend on several organisational and business factors, however, based on the input from the respondents, there is an understatement about the ability in balancing the capacity planning for maintaining operational tasks with the need of scaling up resources if a serious incident hits the business. We would argue for the need of establishing an organisation-wide risk management process to align the organising of a SOC with the business goals. According to InfraCERT, "Do a risk assessment and mapped which value chains you have and what the core business is..." (R6), would help the business understand the importance and purpose of having a dedicated security team working with monitoring and detection activities.

"...most effective will be to have an internal incident response function or a CSIRT..." (R6)

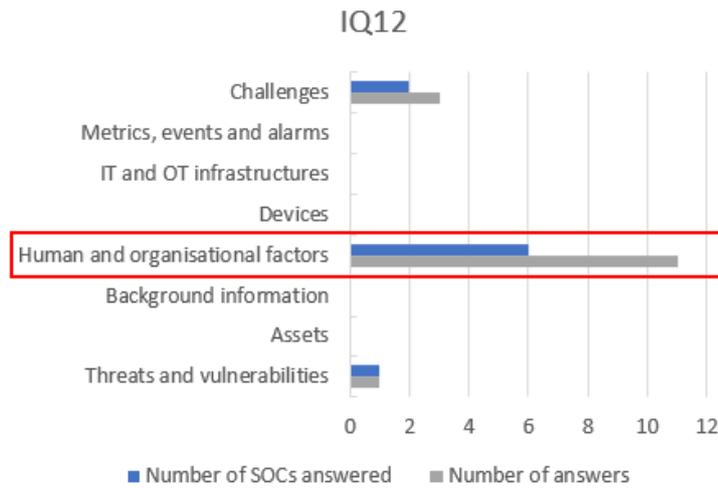


Figure 4.14: Security Operation Centre mapping of themes for IQ12

4.5.4 IQ13

For IQ13, "What type of SOC operating model should be used for IoT?", we have asked a concrete question regarding the operating model and what would fit for security monitoring IoT devices. The concept of an operating model for a SOC represents how an organisation would orchestrate its capabilities to achieve strategic business objectives. "An operating model brings the business model to life; it executes the business model." (Gartner, 2023). We have mapped IQ13 with the theme "human and organisational factors" and the RQ3 and collected a total of twelve statements from all six SOCs.

Optimal monitoring should be interpreted as finding the best organisation model for monitoring IoT devices aligned with the business objectives. Organisational factors can be addressed depending on the size of the SOC and operating hours, and the mission. A SOC can be organised using different operating models, from only operating during regular working hours, or around the clock - twenty-four-seven supported by an outsourced managed security service provider (MSSP), or utilising follow-the-sun principal, where several SOC teams from different time zones, can overlap and cover for each other during a day. Equinor has mentioned how they use a hybrid operating model through the statement, "we don't have a 24/7 staffed internal SOC, so we use Mnemonic as an extended arm of us at weekends and in the evenings..." (R2). A hybrid model can be recognised by having both in-house personnel in combination with outsourced security professionals for handling when need for scaling and capacity planning. However, it is important to mention that the responsibility for operating the IoT system and the owner of implied risks are solely owned by the businesses. According to NSM, it is therefore important that "each business assesses itself with a balanced method between human knowledge level and how much the business will own and handle..." (R5). This is also supported by a statement from SIKT that "risk must be assessed for how important this is..." (R4).

Independent of the operating model chosen by the business, when an incident occurs, the incident handling process is core for how long an investigation is and would depend on the business's own resources with a deeper knowledge of system behaviour. This knowledge is vital in an incident-handling situation when important decisions are made to reduce the impact on the business. According to Mnemonic, when the "complexity is so high and the importance is so great

that you have to take this very seriously... this with monitoring... it is very resource-intensive to build this yourself and have control over this..." (R3). However, such a statement would not describe the degree of outsourced SOC supported in an operating model, and according to Equinor, they don't have credibility in an operating model using a fully outsourced SOC model, "I have no faith in outsourcing the SOC – it could be a very expensive lesson..." (R2). The effort of orchestrating and establishing an incident response team under such organisational conditions would likely have a high risk of damaging the business continuity objectives.

InfraCERT has mentioned a worry addressing the competence sharing and lack of communication from a SOC perspective, between SOC, IT and OT personnel, "one thing that I think is very lacking is the link between... we call it SOC... IT and OT security people - and those who operate IoT or operate the SCADA system... those who actually control the electricity or heat production..." (R6). However, the operating model chosen for the business should be challenged to minimise this gap by bridging the SOC's capabilities into the OT domain. A possible future operating model can be a new opportunity to investigate and harmonise the incident handling process between SOC, IT and OT.

"It is important to balance the HTO (human-technology-organisation) perspective..." (R5)

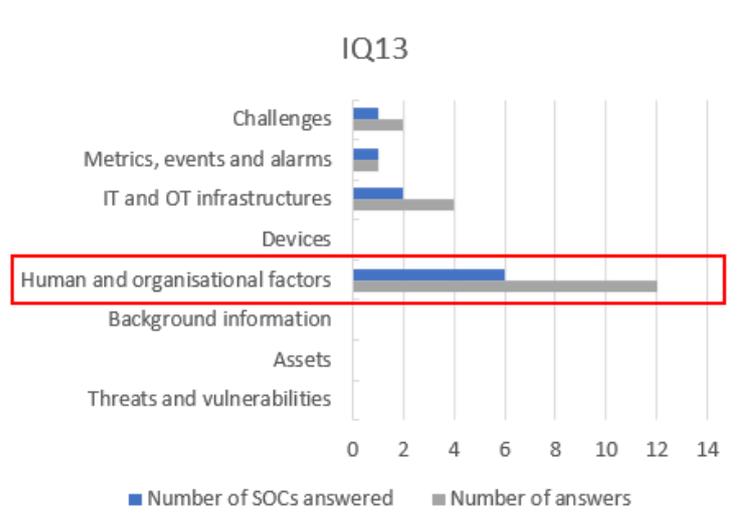


Figure 4.15: Security Operation Centre mapping of themes for IQ13

4.6 A quantitative summary of the result

We have collected and counted in total 499 different statements from the six SOC interviews. In this study, 354 of 499 statements were mapped to themes and used in the analysis to present the answers to our interview questions. Table 4.6 summarises the themes with mapped statements.

Table 4.6: A quantitative overview of the result using thematic analysis to present identified themes with statements to answer IQs.

Theme	Total statements	Mapped and theme used statements
Challenges	118	70
Metrics, events and alarms	83	67
IT and OT infrastructures	104	84
Devices	23	11
Human and organisational factors	70	61
Background information	45	29
Assets	18	17
Threats and vulnerabilities	38	15
Sum of statements	499	354

In total, the number of answers provided by each SOC is presented in Figure 4.16. The highest number of statements was from R2 (Equinor) with 138 statements followed by R1 (IFE SOC) and R5 (NSM) with 134 statements. We collected the fewest from R4 (SIKT) with only 22 statements.

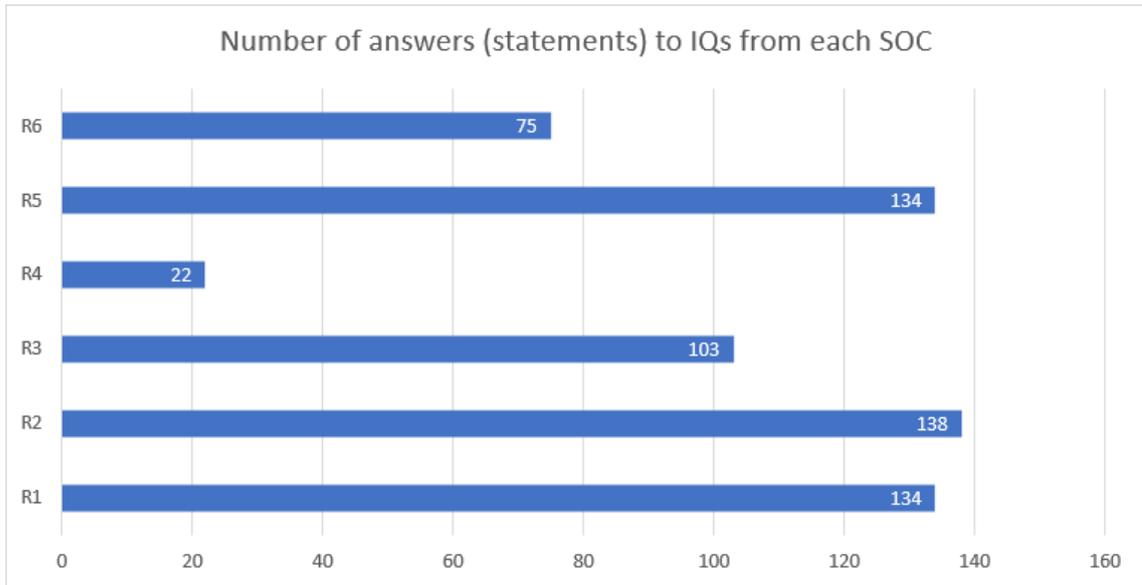


Figure 4.16: Total number of answers (statements) from each SOC

In Figure 4.17 we present how the number of statements was provided by each SOC as answers to the IQs. Here the IQ9, about the use of edge computing, scored the lowest with only 11 statements where 8 of these came from R5 (NSM). The IQs with the most statements provided was IQ8 with 84 statements. If we look at the distribution of the provided statements, we can see less variance for IQ4 and IQ9 where we lack statements from all the SOC.

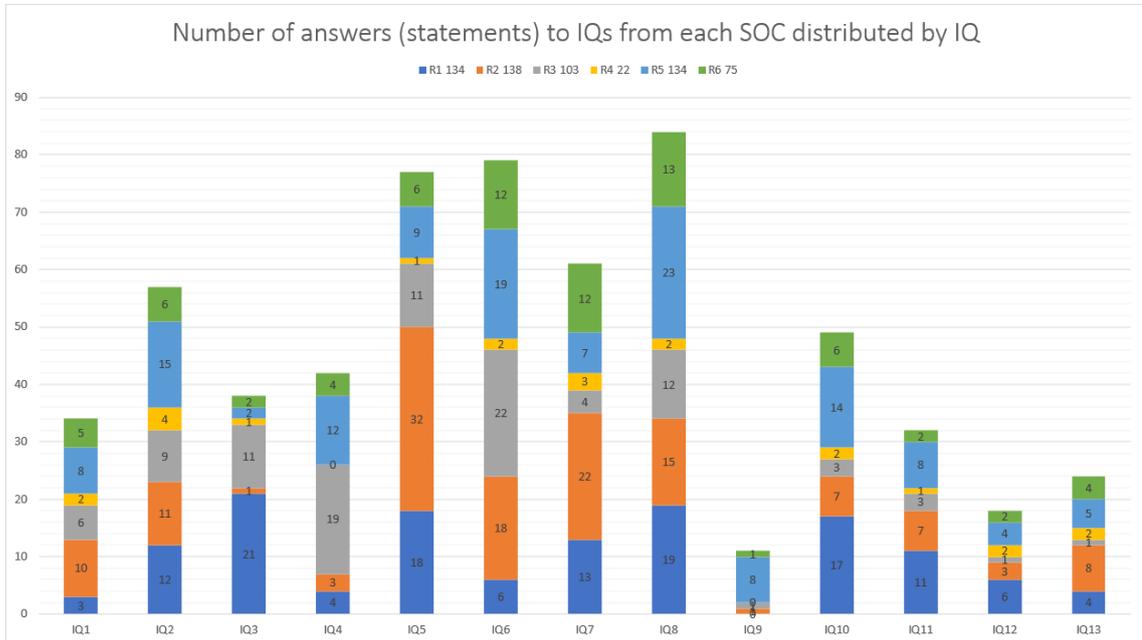


Figure 4.17: Number of answers (statements) from each SOC distributed by IQ

Chapter 5

Discussion

In this chapter, we discuss and reflect on the interview process results. The findings from the results were presented using themes and codes as statements from the six SOC to answer the RQs. In this qualitative research, we discuss and answer the RQs for the validity, reliability and uncertainty of the collected data using the "Consolidated criteria for reporting qualitative studies (COREQ)" (Tong et al., 2007, p. 352). The COREQ checklist was used as a guideline for how to report on qualitative data, after conducting semi-structured interviews, using the 32-item checklist with questions. The checklist has several questions distributed over three different domains, addressing the research team (1) that conducted the interview, the chosen study design (2) and the analysis and findings (3). The checklist with questions was answered and provided in Appendix D.

5.1 RQ1: What are the challenges in security monitoring, maintaining and operating IoT devices?

In today's society, we are surrounded by technologies and innovations using IoT devices connected in many ways from single communication lines to being part of larger distributed systems. IoT usage is within many domains and businesses. We know from the state of art literature and findings, that cheap IoT devices that have low computing capacity were often exposed to poor system designs with a lack of security in mind. This could potentially introduce new risks for the business. When addressing the IoT challenges we need to provide some background information from the field of operation. In an ideal monitoring and operation situation of IoT devices, we should have all the devices enrolled in an IoT framework for continuous monitoring with health and performance indicators, management tools for updating and patching and operators with competencies from both the IT and OT domain, to mention some. However, this ideal operating model has been proven to be challenging to establish in practice.

To answer the RQ1 and the two sub-RQs 1.1 and 1.2, we considered the theme "challenges" and statements mapped in Table 3.4 for IQ3, IQ5, IQ7, and IQ12. A map of these challenges was analysed and presented in Figure 5.1. In Appendix E we have in Figure E.1 expanded the statements for each category from the theme "challenges".

5.1.1 Security monitoring

One of the important tasks of a SOC function is security monitoring, which is about automating the process of collecting data and analysing activities from devices and networks to discover

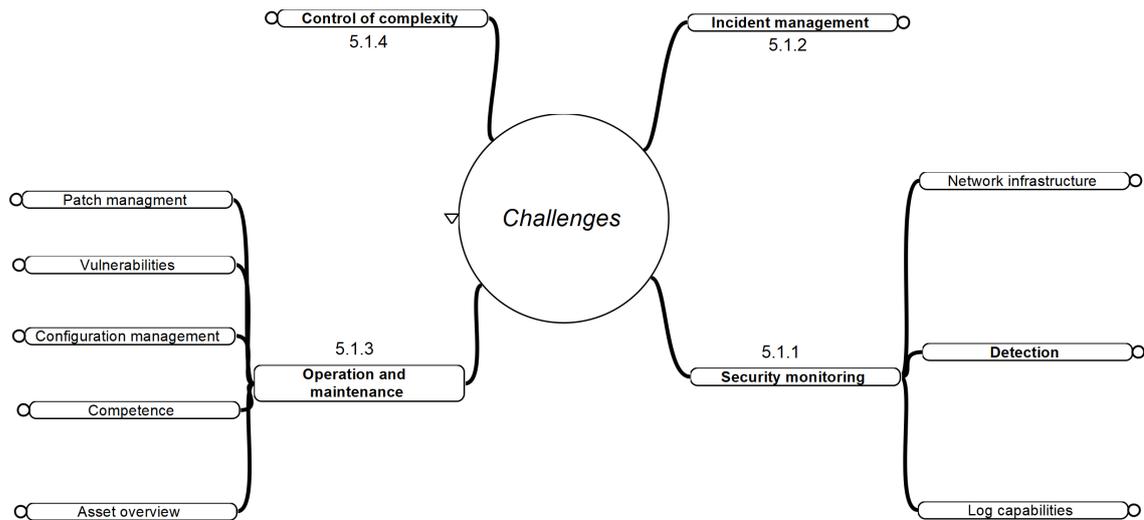


Figure 5.1: The map of SOC challenges for IQ3, IQ5, IQ7 and IQ12 addressing logging, monitoring, detection and operation within the IoT-, OT- and IIoT domain.

vulnerabilities and anomalies and act upon the current situation. One of the main challenges faced by the interviewed SOCs was related to security monitoring, logging capabilities and detection. This was closely connected to the fact that IoT devices generally have fewer computing capabilities to do other operations than the designed purpose, gathering data from a sensor or controlling an actuator. When considering security monitoring, we first need to address the availability of information and data to collect. The different device's logging capabilities are dependent on the availability of logs. Logs were mentioned to be the number one source of event information for monitoring IoT devices. However, that would not be of any use if we cannot find it or forward it to a central logging service in a monitoring solution for further insights and analysis.

Log capabilities. We have during the interviews found several statements from the SOCs, claiming not to have proper data from devices. The lack of logging capabilities at the device level was mentioned, and according to InfraCERT (R6), "very few have the opportunity to send logs you actually need" (R6). IFE SOC (R1) has experienced that it is "challenging to monitor endpoints and sensors" and that "the IoT problem is partly that it is proprietary and then there is not so much focus on getting out the parameters you need to be able to monitor". A general challenge and observation from the different SOCs were that "the problem is to get information out from the devices" (R1). With less information and data to retrieve from the devices, we often seek other solutions for insights and look for communication carriers and where the device is connected in the network infrastructure to find complementary information about devices and their behaviour. Another source of information is the network traffic which we can provide metadata and information from the network protocols in use between devices. However, according to NSM (R5), the challenges were "IoT devices that has no security in the component structure in relation to the OSI layers"¹ (R5) because they were constructed simpler and for dedicated purposes without security or logging capabilities in mind.

Network infrastructure. The different SOCs have mentioned several challenges originating from the underlying network architecture and have shared concerns about heterogeneous networks and fixed networks leveraging communication with many different devices. NSM (R5) has mentioned that they have experienced IoT devices where "it is not intended that it should

¹The Open Systems Interconnection (OSI) network reference model

be possible to secure the protocol on which it communicates" (R5). Equinor (R2) and Mnemonic (R3) were quite aware of their operational responsibility and focus for managing OT networks with different levels of criticality depending on the type of network and device types. The most critical networks consisted of ICS devices that were subject to challenges regarding which method to use for retrieving information from networks without interfering with the business process operation. Hence, these networks cannot have downtime and the method of passive network monitoring where used for this purpose. This was mentioned by a statement provided by Equinor (R2) "if you create a little queue in the network, you will get production shutdown" (R2). According to Equinor (R2), "technically challenging it is... e.g. protocol understanding on passive network inference" (R2) was used as we cannot probe or do active monitoring to retrieve information from OT devices. This concern where more about the concern of risks making a queue in the network that could potentially interfere with the data gathering and communication processes of the process control network. Security monitoring is part of a holistic view of security and measures for protecting such networks and according to Mnemonic (R3) "segmentation is absolutely essential" for protection by dividing the networks into smaller parts and placing similar devices with the same communication patterns into similar groups of devices.

Detection. Detection is a part of security monitoring where we filter out irrelevant event information and defined known conditions, patterns or thresholds for events regarding device behaviour where we want alerts. These alerts were subject to take action. However, detecting anomalies where mentioned by Mnemonic to be "the biggest challenges - discovering abnormal things that are happening" (R3). From the OT network perspective, several challenges addressing detection specifics were mentioned. The "lack of protocol parsing support" (R2) for industrial protocols was mentioned by Equinor as a challenge when interpreting commands sent in the network for understanding and creating detection patterns. This becomes like a paradox when we consider the enterprise level and the IT part of the network where we often want to encrypt the network traffic. Hence, the opposite situation applies to an OT network where "encryption will only harm the possibility of detection, as we lose insight into what is happening on the network and the attacker" (R2) and was mentioned by Equinor (R2). We must also take into account that these OT networks were well controlled, protected and supervised considering changes or abnormal behaviours as mentioned previously. With fewer monitoring parameters and information available from equipment and devices, there were challenging to make good detection patterns. The cause of fewer logs causes difficulties in the detection of anomalies and the quality of triage of events for alarming.

5.1.2 Incident management

A SOC should work proactively to reduce the likelihood of a possible impact from the perspective of threats and vulnerabilities and how this relates to the business and the system environment. A risk-based approach on how to handle incidents with certain criticality would be of high importance for a SOC to consider when there is a need for acting reactively in situations to handle a security incident that has occurred. Doing the right thing by prioritising and containing affected systems to minimise the potential impact would be essential for minimising downtime and production systems hazards. Every planned or unplanned organisational activity would be valuable information for a SOC to know about in conjunction with the status of devices and the current system landscape concerning threats and vulnerabilities. This builds up what we call a situational awareness of what was expected behaviour of changes and deviations from the normal operation. We have gathered statements from two of the SOCs who have mentioned that there

were challenging to maintain an updated overview of an operational situation. This relates to the statement shared by IFE SOC (R1) that "for a SOC, it is challenging to keep track of everything" with several systems in a monitoring solution the complexity of managing an incident becomes challenging. Mnemonic has mentioned that "the more such systems you put into a monitoring solution, the larger that matrix becomes" and the incident management process for handling unplanned events that can affect the system operations becomes a challenge. The risk-based approach would be to avoid or delineate devices by placing them into a separate network for gaining better control of the network traffic. According to IFE (R1) "if you don't have full control over what they are doing - it's usually a bit like "black box" solutions" when having unknown devices in operations.

5.1.3 Operation and maintenance

A **SOC** is a specialised team within an organisation that has the mandate to protect and handle security incidents. Establishing a monitoring regime is challenging and it is hard to get a holistic overview of all devices and know what types of devices you have in an organisation and operation. To address these challenges we were dependent on closer collaboration with the teams working with **IT** and **OT** operation and maintenance sharing operational issues and maintaining device definitions through a common asset register with the **SOC** team.

Asset overview. According to IFE SOC, it is "hard to get an overview" (R1) and we have discussed that systems have different criticality that would prioritise how security events and alarms were ranked according to how incidents are handled by a **SOC**. We have the complexity of the legacy systems on one side, and on the other side, new systems are introduced into the same systems landscape with different criticality and with few monitoring requirements. This was linked to the challenges of having an updated asset register to "know what device you have" (R1). A system overview with an asset inventory including the relationship between devices, components and criticality is key to setting the mode of operation in a **SOC** in line with the business goals. The SOC's scope of responsibility should, however, always reflect the current threat landscape.

Configuration management. Hence the need of having tools with management capabilities to maintain an up-to-date fleet of devices is essential. The challenge of maintaining a set of configurations with security controls for hardening purposes requires device capabilities to be enrolled into a system for controlling and managing devices. With this in mind, we know from history, that **IoT** devices in operation, potentially could have unveiled critical vulnerabilities that would require rapid patching and control over vulnerable devices. However, this would require new approaches and tools from design specifications to applied products when there were fewer devices with remote update capabilities for management. From an operational and management standpoint, the lack of device management tools with security monitoring parameters capabilities would be a requirement when addressing and developing more resilient networks and devices in the future. **IoT** devices and legacy systems that were part of a management system in operation become a challenge in the future when security measures need to be applied.

Vulnerabilities. In an operational context, we have to consider the possible attack surface of having unmanaged and un-patched **IoT** devices in operation. This problem becomes more severe and unmanageable, if not taken into account for the possible risk introduced by unwanted device events to occur. According to Equinor, they face a challenge when it comes to identifying vulnerabilities in the different systems, "We simply do not have the capacity or maturity to look at vulnerability management quite yet..." (R2).

Patch management. The maintenance window where utilised for patch management and was mentioned to be an ongoing task with regular rounds of checking the different devices where some systems were product specific and would require the involvement of suppliers planning for upgrades. In such cases, an updated asset overview becomes handy if the information about the current security patch level were updated. This was also mentioned as a challenge for having personnel with competence available when "you do not have expertise in all the systems, so you are very dependent on the suppliers" (R2).

From a life cycle management perspective when operating and maintaining systems with different device types there were some distinct differences between IT systems and OT systems on how long these systems would be in operation. When we consider an IT system the lifetime would often be around 3-5 years before the system is off-boarded or decommissioned. However, when we consider systems that were developed for the industrial side to operate or control critical or semi-critical processes the lifetime of such systems were often considered around 15 to 30 years of operations. Without security in mind from the early stages of the development cycle, such systems become hidden and suddenly vulnerable to new threats. With legacy systems in operation, this would require knowledge of the existence and behaviour of the system with the competence to manage and address this challenge.

Competence. The complexity of operating critical systems in production were mentioned as a challenge when there was a need to scale the organisation's capacity with personnel and competence to address vulnerabilities in systems. The operational organisation rely heavily on the supplier's capabilities to provide and backfill with the necessary competence. According to Equinor (R2), they were "in practice depending on the suppliers giving the thumbs up. It is a very big challenge" when planning maintenance tasks for changes like applying security patching of systems. From an operational view building the needed competence require dedicated personnel working closely with these systems knowing how they behave during different conditions and being able to distinguish between an operational event and a security event. According to Mnemonic "very much of the context around this requires you to work with this at all times... it is in a way a challenge" (R3) and builds "product specific" (R1) competence for the most mission-critical systems. In line with these statements, there was also referred to a competence gap challenge frequently mentioned by the SOCs. The SOCs cannot have competence in all kinds of systems and must rely on suppliers for refilling with competence. However, for a SOC this could be self-knowledge and according to Equinor "it is a fact that it is demanding to be good at both OT and IT" (R2) when improving the monitoring situation of these systems.

5.1.4 Control of complexity

The overarching system complexity of operating and monitoring mission-critical systems has been mentioned as a challenge. Establishing a security monitoring regime for devices and systems being resource-demanding both in time and competence, and we have heard about the availability of skilled personnel to be limited in complex operations if we consider these OT systems operating 24/7. Equinor has mentioned that there is a challenge in planning for changes or applying needed features inside control systems and networks for improving the insight of data regarding security monitoring. The complexity of maintaining many different sub-systems with a diversity of device types and vendors requires careful planning and extensive supplier support. In addition, maintain up-to-date operational documentation with changes. The practical consequences mentioned have been that the *rate of changes* increases as we have to consider safety and security aspects in

complex systems and organisations. Equinor has shared that they were "very far behind when it comes to OT so you have a big backlog" (R2).

With these statements, we have provided the current challenges to answer RQ1 and we would agree that there still is a need to address these security monitoring challenges. There is a need for the adoption of standardised device specifications with security and monitoring capabilities to close this gap. There is still a need to gain more data from devices and networks both from mission-critical and non-critical systems.

5.1.5 The SOC's perspective on IoT security monitoring

To answer the **RQ1.1: What is the challenge seen from SOC's perspective on monitoring IoT devices?**, we consider the previously mentioned statements regarding the lack of management capabilities of IoT devices and systems.

From the results provided in Figure 5.1 we can conclude that there were still several challenges in monitoring IoT, IIoT and OT devices. There was even a problem of knowing their existence, especially when considering IoT and IIoT devices, which can be surprising for a SOC. The known awareness about IoT devices was lower than we expected from the different SOC's. However, we still know that unmanaged and unpatched devices can be a vector for elevating access to back-end infrastructures. This could indicate that there is a low maturity level and an absence of IoT security monitoring practices within the IT domain. This could be related to what InfraCERT mentioned about simpler IoT devices in use were "usually on the non-industrial side, it's more like 'set-and-forget' they sell them and then they are no longer supported..." (R6). When it comes to the OT part of the infrastructure, we experienced that established SOC's with a long history of operation of ICS and OT networks were already in a setting and practice with limited security monitoring of IoT devices. Hence, the availability aspects of critical systems overcome the risk appetite for the frequent need for management and patching of known vulnerabilities.

Another aspect of security monitoring was the insatiable need for more data to develop better detection scenarios, and according to Equinor the SOC personnel describes they use "most of my time or 80% of my working day, is not about detection, but getting enough data in..." (R2). Querying for event information from logs is an important source for creating detection for alerts. With centralised logging and more storage and computing power, we can make more complex queries and logic to detect techniques and tactics originating from possible attacks. A general opinion by the SOC's regarding IoT devices monitoring from log sources where that "simpler IoT devices do not have that option because they have been constructed simpler" (R5). Even though, "the biggest challenges - discovering abnormal things that are happening..." (R3). The previous statement was more related to what Mnemonic indicated as "very much of the context around this requires you to work with this at all times... it is in a way a challenge" (R3). According to Mnemonic, "the more such systems you put into a monitoring solution, the larger that matrix becomes..." (R3) and the scaling of the SOC function for an optimal operation can also become a challenge.

To answer the **RQ1.2: What is the state of practice for monitoring IoT devices?**, we have considered what has been shared by the SOC's on how they manage and practice IoT monitoring. Today's focus on security monitoring were mainly based on network traffic. Within OT networks and process control, network security monitoring was mentioned by Equinor, Mnemonic, InfraCERT and NSM as a method used for passive monitoring of the network traffic. Passively means that we collect information available from the network to "detect vulnerable network services without having to scan the devices" (Stouffer et al., 2022, p. 124). Using this approach requires minor changes to the network equipment and it is easily available and does not intervene with the system

processes running on critical devices or devices with low resources. A central passive network monitoring is mentioned as a convenient method used in monitoring, as "you cannot make active queries on the networks..." (R2) with the risk of creating a queue in the network.

However, this would be the case for business-critical OT networks. The use of network monitoring can also be a direct consequence of having fewer logs and health monitoring options available. Within the enterprise network on the IT side, we register more maturity and device log capabilities within the SOCs for retrieving additional logs from other types of devices which would provide a correlation between log sources when working with detection. The use of network monitoring in combination with network logs and performance metrics from endpoints where more widespread practice within environments with less critical processes, like the IT enterprise networks. However, the challenge provides the opposite practice regarding monitoring when very few have the capability to forward logs to a central logging service as a result of a lack of security monitoring of IoT devices.

Not having an IoT device in a monitoring regime forces other methods and approaches for data gathering. With the risk of causing a potential negative impact on the business network. The assumed breaches were a new approach coming from the Zero Trust initiative that has been mentioned by InfraCERT and NSM as a method of inverted trust of devices connected to the network without proper authentication and verification of a device's legitimacy.

We should work towards the assumption that we will discover vulnerabilities introduced by IoT devices also in the future. IoT devices operating within heterogeneous networks, constituted by many different types of devices and closed ecosystems, were more likely to be excluded from the monitoring regime by a SOC. However, having this knowledge the role of SOCs should prepare for handling the massive amount of IoT devices. The SOC have a challenge in bridging the gap between IT and OT with limited mitigation options for IoT devices, both in regard to criticality aspects for containing an OT system, but also when we consider available techniques for containing IoT devices without taking them out of production.

5.2 RQ2: What type of data is collected from IoT devices to detect anomalies and what information does this relay on?

A SOC's monitoring and detection capabilities depend on the available information gathered from the underlying infrastructure and devices for use in anomaly detection. To answer the RQ2 and RQ2.1, we have considered IQ4, IQ6, IQ7, IQ8 and IQ9 from Table 3.4 for the themes "metrics, events and alarms", "IT and OT infrastructure" and "devices". Only the theme "metrics, events and alarms" was considered relevant.

There was less information shared about specific device information and how these were handled concerning data collection that could enrich the security monitoring context considering the themes "devices" and "IT and OT infrastructure". However, we have included all the themes maps in Appendix E. In Figure E.4 we have expanded the statements for each category from the theme "metrics, events and alarms".

We have found statements and categorised them within "security information" and "detection" for the theme "metrics, events and alarms", and we will use this information to discuss how anomalies are used today for indicators with respect to detection. The practices used by the industry as the basis to make anomaly detection were mainly taken from the theme "metrics, events and alarms".

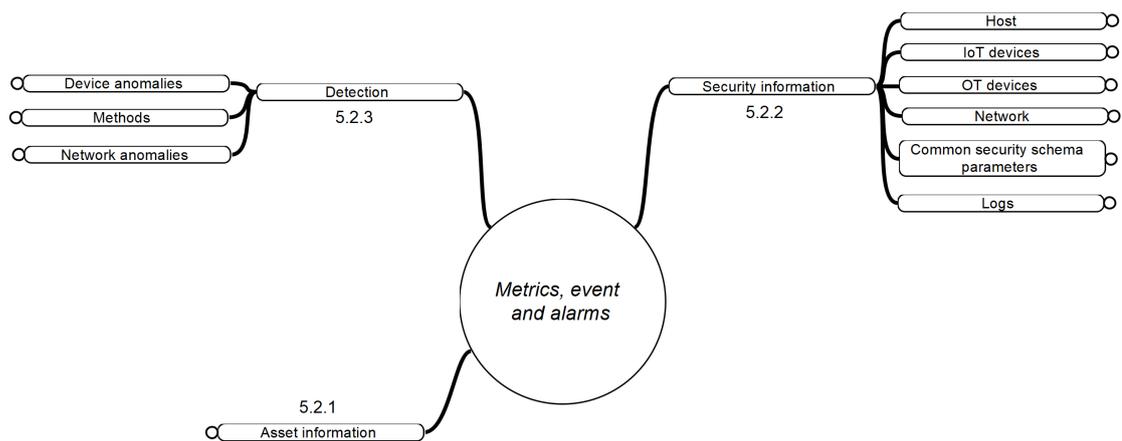


Figure 5.2: A map of metrics, events and alarms statements for IQ4, IQ6, IQ7, IQ8 and IQ9 addressing IoT management, monitoring and detection from the IoT domain.

In the theme "metric, events and alarms" in Figure 5.2 we have found security metrics from devices and networks shared by professionals in the field of security operation (SecOps). NSM (R5) and InfraCERT (R6) have mentioned that detecting how a device moves in networks and between infrastructures was important for detecting lateral movement (NCSC, 2023). Lateral movement is one type of tactic a threat actor could engage with for moving deeper into the network to find other vulnerabilities and weaknesses for elevating privileges and persistent access. This type of anomaly behaviour would require monitoring parameters collected from the underlying network and correlation with security information from endpoints and devices.

The respondents did not mention any specific tool, but a security information and event management (SIEM) tool is a prerequisite for a SOC to collect and store logs and event information from equipment like routers, network switches, firewalls, endpoints and intrusion detection systems (IDS) inside the infrastructure. According to Gartner, a SIEM solution is a technology that "...supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources." (Gartner, 2023). Early detection of abnormal behaviour is key to maintaining the resilience operation of a business.

The MITRE framework is an established source of knowledge with the description of "adversary tactics and techniques based on real-world observations." (MITRE, 2023a). The ATT&CK model is divided into three different technology domains (E. Storm et al., 2020, p. 8) where the first (1) represents enterprise networks and cloud technologies and is named MITRE ATT&CK® Matrix for Enterprise. The second (2) domain is a matrix for mobile communication devices and the last (3) represents the technology domain for industrial control systems and is called MITRE ATT&CK® Matrix for ICS. The MITRE ATT&CK® Matrix "covers documentation of adversarial behavior during requirements gathering, reconnaissance, and weaponization before access to a network is obtained" (E. Storm et al., 2020, p. 8) and is a method used to describe a threat actors tactics during a cyber-attack operation. According to MITRE, techniques are actions performed "into more specific descriptions of how behavior is used to achieve an objective" (E. Storm et al., 2020, p. 9) and with these two describes the specific implementation of techniques into procedures. Tactics, Techniques and Procedures (TTP) is a concept describing threat actors based on the pattern of behaviour, processes and tools are used for their actions. According to NIST, the TTPs are used by security professionals to describe the highest level of a threat actor's behaviour (C. C. NIST, 2023).

The state-of-art from Chapter 2 was mainly based on research and academic papers and had less information about practices in implementing guidelines taken from standards and the established cybersecurity frameworks. NIST contributes to standards, guidelines and best practices and the same applies to MITRE which has contributed to a better understanding of technical attack techniques and the threat actors' behaviours.

In table 5.1 we have interpreted and categorised statements from the respondents relevant to describing the current situation of available information within security monitoring. However, this overview was not extensive with respect to actual usage but will give an introduction to examples of security metrics and events with use cases for anomaly detection.

Table 5.1: Data collected and analysed from the theme "metrics, events and alarms" with indicators relevant for anomaly detection.

Metrics, events and alarms	Asset information	Device identification					
		Functionality					
		Network connected to					
		Which network is the device connected to					
		Operating system					
		Version of operating system					
	Security information	Host	IoT device	OT device	Network	Logs	Common security schema parameters
		Running processes	Alive and responding normally	Commands sent	Number of packets	Central logging	Uptime
		CPU load	Packets resent	Commands received	Type of network		Device integrity status
		Disk space available	Type of data sent	PLC upload	NetFlow		Type of data collected (classification)
		Memory usage		PLC download	CPU load		Properties
		List of previously used wireless networks		Communicating partners	Memory usage		
		OS events			Network link changed (up/down)		
		Connected USB devices					
		Logged on users					
	Detection	Methods	Device anomalies	Network anomalies			
		Passive network monitoring	Detect all variance in behaviour	Amount of data between peers			
		Use network traffic thresholds to identify normal and abnormal behaviours	OT network alarm for any strange behaviours	Fixed network with expected traffic patterns			
		Integrate with external threat intelligence sources to create playbooks for mitigations	Detect device behaviour in the network	To much traffic			
		Physical alarm and lights	Detect device not responding	To less traffic			
			Detect device movement in networks				

5.2.1 Asset information

Updated history and current information about the assets were mentioned by the SOCs to be useful in an incident handling process to help distinguish between operation events and security events. A general observation from the interviews was the respondent's talk about the need for contextual information about devices and systems to perform a quick response to an incident. Every piece of information that could enrich the context was mentioned to be helpful. However, in particular, having an automated and updated inventory of all assets of every business value chain is perhaps not feasible in practice, as this also would require active polling of the information from mission-critical instruments and devices.

Defining a minimum viable asset information could benefit the incident management process for the SOC team. The asset inventory register is not complimentary but should have a unique identification of devices with a description of their functions. In addition, information about where the device is connected in the infrastructure with versions and types of operating systems was mentioned which could enrich the context. The next question would be to identify which type of security information would be relevant.

5.2.2 Security information

Equipment and devices have different data and information that could benefit security monitoring in detecting the abnormal. **Host**-based information about running processes with CPU load, memory usage and available disk space would indeed be classified as operational data. However, such operational metrics would enrich the interpretation of the security events from the operating system (OS) with performance data to help describe a system's behaviour. This would not be fully complementary information. However, the respondents have mentioned for example using OS events to create detection rules when connecting USB devices to a host that could indicate a technique for initial access by replicating access through removable media (MITRE, 2023b).

Another example shared was the detection of wireless attempts to use other wireless networks that are normal by retrieving a list of the previously used wireless network profiles from a host. According to MITRE, such behaviour could be an indication of "a method of gaining communications and unauthorized access to a wireless network" (MITRE, 2023c). Depending on the role or function of a typical host when creating detection rules we can use information based on a known list of users to be present on a system. Anyone else who was logging on would generate an alarm and would be subject to further investigations.

Security information mentioned useful with regards to **IoT devices** is to know if a device is alive and responding as normal. This information would be based on network packet metrics like the number of packets sent or received with some identification of types of data transmitted. For **OT devices** information about which commands that were sent and received by the PLC in a normal production setting would be beneficial and could be used for detecting anomalies. However, such data need to be correlated with other operational data with regard to maintenance windows or the urgent need of managing maintenance work. We know from earlier observations that any irregular concerns about mission-critical OT devices could generate alerts because of fixed network environments with less information to make granular detection for specific devices in regard to abnormal behaviours. A PLC download or upload command (mentioned especially by Equinor) is of interest to be detected as this would have a huge impact on the physical process and the environment if something could influence the PLC logic. Therefore, having a quick overview of who or which device has been communicating with the PLC becomes a piece of important context information when dealing with alarms in a SOC.

The underlying infrastructure has additional security information that could complement necessary device behaviour. The number of packets, switch interface changes, type of network and network switch performance indicators like CPU load and memory usage would provide additional context. The use of NetFlow data provides insights into the details of the internet protocol (IP) traffic between communication partners to measure types of services and packets with byte counts. According to CISCO, the Netflow data could provide vital information "...used to efficiently allocate network resources and to detect and resolve potential security and policy violations" (CISCO, 2023). Nevertheless, we can see the need for a minimum viable **common security schema** for IoT devices that summarises all security parameters like uptime, device integrity, etc. across device types. All these different data sources and **logs** with information can be fed into a SIEM solution for central logging and querying to create detection rules for specific purposes. However, every data mentioned here were based on known patterns and would not be complementary in every situation.

5.2.3 Detection

As every system is unique with respect to its performance and to some extent the known behaviour we continuously need to hunt for data with pattern conditions to detect anomalies in networks and devices. **Methods** and techniques that were mentioned used was *passive network monitoring* to utilise the network traffic to identify metrics and thresholds for what is expected to be normal network traffic patterns to detect any anomalies. The development of patterns and conditions for a system based on collected data can be challenging with respect to competence and knowledge. External threat intelligence services can be a useful source to extend product-specific indicators to detect patterns developed by vendors or others. We have already mentioned several typical **device anomalies** with lateral movement and **network anomalies** for continuously measuring the network traffic for improving the detection.

However, we should not be over-enthusiastic about improving the detection rate of possible abnormal behaviour too much. The number of alarms triggered detection patterns based on poor quality or fewer data available would be impossible to manage and handle in practice when working on identifying security events and solving security incidents. Warnings and alarms generated from many systems on suspicious activities and events can be overwhelming to handle in practice. These types of behaviour in a SOC setting were often called "alarm fatigue". These experiences were shared by InfraCERT (KraftCERT) with a concern about the fact that "alarm fatigue is very real there are so many alarms" (R6).

To answer the **RQ2.1: What type of remediation methods are used to mitigate IoT security alarms and incidents?**, we did not find any relevant techniques mentioned by the SOCs for IoT device remediation. There were fewer practices shared. The adoption and awareness of IoT devices for security monitoring were lower than we expected. In addition, there were no experiences shared by the SOCs about how to manage and handle IoT security incidents in particular. However, we assume that such incidents would be handled according to existing techniques used on the endpoint by containing or quarantining devices by taking them offline or isolating the network segment for further spreading.

5.3 RQ3: How should SOC's operate and work in the future to adapt to monitor the increasing number of IoT devices?

We have previously mentioned the SOC's journey towards the continuous hunt for more logs and monitoring conditions of IoT ecosystems and devices. Through the themes "assets", "threats and vulnerabilities", "human and organisational factors" and "background information" we seek to find new knowledge about how a SOC introduces IoT devices for security monitoring. A SOC should prepare for its future journey of operations and efficient incident handling to mitigate potential threats against IoT systems. We have considered statements from the previously mentioned themes to find answers for RQ3 using the mapping of IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13 in Table 3.4. Based on the result we will mainly focus on the themes "threats and vulnerabilities" and "human and organisational factors" to answer RQ3 and RQ3.1.

We have seen from the industry respondent's statements the use and the vague awareness of IoT devices and the system's existence for different purposes. The level of awareness and insight into IoT devices and ecosystems was mentioned to be very limited in establishing a monitoring regime of these systems. At the same time, we have an evolving threat landscape to follow that puts pressure on established SOC's. With a future expectation to extend monitoring capabilities of proprietary and specialised IoT systems, it is hard to keep up with the pace of work to improve and reduce the risks of impact on the business. However, there was one significant difference that we want to mention about the awareness of IoT- and IIoT- versus OT devices. The established SOC's like the one with Equinor and Mnemonic which operate and monitor OT systems have a more clearly defined objective regarding security monitoring of mission-critical devices.

However, we have mentioned challenges that every business has in common with regard to the emerging threat landscape and which covers any type of business and type of device with vulnerabilities that can be advantaged. After the Russian invasion of Ukraine in March 2022 the geo-political situation and tension in the cyber domain increased (European Union Agency for Cybersecurity., 2022, p. 40). We will discuss RQ3 in light of the current threat landscape and how a SOC should prepare for handling the increased number of devices with a focus towards more automated response strategies.

The statements from the theme "threats and vulnerabilities" were further categorised in Figure 5.3 into weaknesses, system impact, and business impact. In Appendix E we have expanded the statements in Figure E.6 for each category from the theme "threats and vulnerabilities".

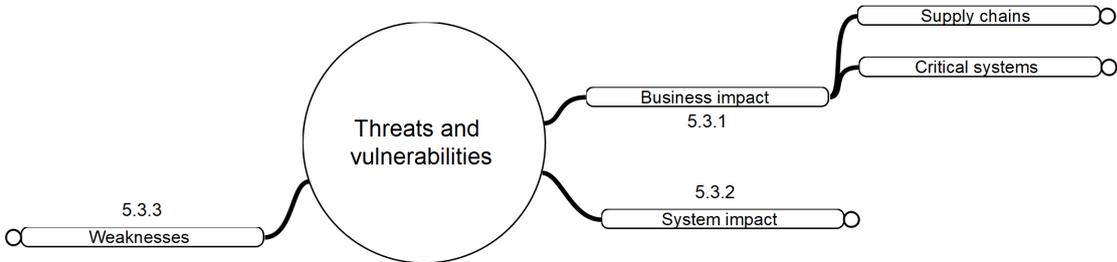


Figure 5.3: A map of threats and vulnerabilities statements for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13 addressing business drivers, monitoring and detection, and SOC from the IoT domain.

5.3.1 Business impact

The business impact from threats and vulnerabilities was about balancing the risks introduced by IoT devices and the consequence of where we place such devices in the infrastructure. **Supply chains.** Along with an increasing number of IoT devices we know that new threats and vulnerabilities will be uncovered in the future system landscape. The story about Ripple20 (JSOF, 2020), was mentioned by NSM during the interview, as one of the major threats to businesses using IoT devices. The Ripple20 vulnerabilities were one example, discovered back in 2020, that unveiled and demonstrated twenty (20) critical vulnerabilities. These vulnerabilities had a major impact on devices using the low-level TCP/IP² communication protocol library from a vendor, named Treck³. Several major device vendors have widely used the Treck TCP/IP protocol library, supplying and supporting many companies with their product development. The vulnerabilities were spanning from products in healthcare, and manufacturing to retail (Santos, 2020), to name a few. The library introduced critical vulnerabilities that opened devices for remote code execution (RCE) and information exposure from devices like IP cameras, networking equipment, printers and Industrial Control Systems (ICS).

Critical systems. Still today, new vulnerabilities were found originating from this vulnerable library and are seen in products widely deployed throughout our society according to the Known Exploited Vulnerabilities (KEV) catalogue maintained by the US Cybersecurity and Infrastructure Security Agency (CISA) (KEV, 2023). These vulnerabilities were also seen in critical systems. A recent cyber security advisory from ABB describes the Ripple20 impact on products used for energy distribution and automation (ABB, 2023). These challenges, combined with the capabilities for maintaining and operating the IoT systems landscape, we face that "very few have the possibility of remote updating..." (R6) according to InfraCERT. With devices connected directly to the Internet without any layers of protection make the Ripple20 vulnerabilities possible to exploit. Hence, the recommended mitigations were not exposing such devices to untrusted networks.

5.3.2 System impact

The increasing number of IoT devices without a life cycle management approach have demonstrated that we must assume that such critical security flaws also may be unveiled in the future. The lack of capabilities and processes for a life cycle management of devices is a challenge that still needs to be addressed and is faced by established SOC's as a challenge. However, establishing processes has less technological focus and is more related to softer elements from an organisation's point of view and addresses the people and processes perspective.

A SOC is often the main responsible for establishing and maintaining the monitoring process of networks and devices in an organisation. The establishment of processes to streamline the operations of IoT devices is challenging to set up because of the diversity of different types of devices that would require an approach for applying different security monitoring profiles. Again, this would require management tools for maintaining and automating the orchestrating of IoT devices for security profiling. Tools having these capabilities were not mentioned to be in use by the SOC's today. Nevertheless, we rely on event data and information available from logs to achieve proper security monitoring. "A log is a record of the events occurring within an organization's systems and networks." (Kent & Souppaya, 2006). Logs are still an important source of information to be analysed by a SOC.

²Transmission Control Protocol/Internet Protocol

³<https://treck.com/>

5.3.3 Weaknesses

In general, a large amount of IoT devices was not designed to log using proper security parameters, and as stated by InfraCERT "very few have the opportunity to send the logs you actually need.." (R6). Therefore it is difficult to put devices into a logging functionality. Maintaining and operating IoT devices over time is essential to build knowledge and sense-making of the behaviour of these devices. From a device perspective, we experience that the default configuration settings for activating logging are often disabled. Activating proper logging can be a complex task and requires special competencies and knowledge involving suppliers and the business unit's IT- and OT personnel. However, this should be a prioritised task in combination with applying a minimum of security properties as identified in RQ2 and with the level of insight into every asset connected to the network infrastructure.

5.3.4 Operational model for IoT security monitoring

In the Figure 5.4 "human and organisational factors" theme, we discuss the organisational structures together with how the organisation interacts with systems and humans when we consider the behaviours both on an individual and team level. In Appendix E and Figure E.5 we have expanded the statements in Figure 5.4 for each category from the theme "human and organisational factors".

The three pillars; people, process and technology are well-known in cyber security as success factors when considering how an organisation performs when working with, implementing and operating IT/OT systems. In a future security operating model, the equal balance between the three pillars comprises the golden triangle in cyber security and comprises the foundation of how a SOC make a difference by being a learning organisation.

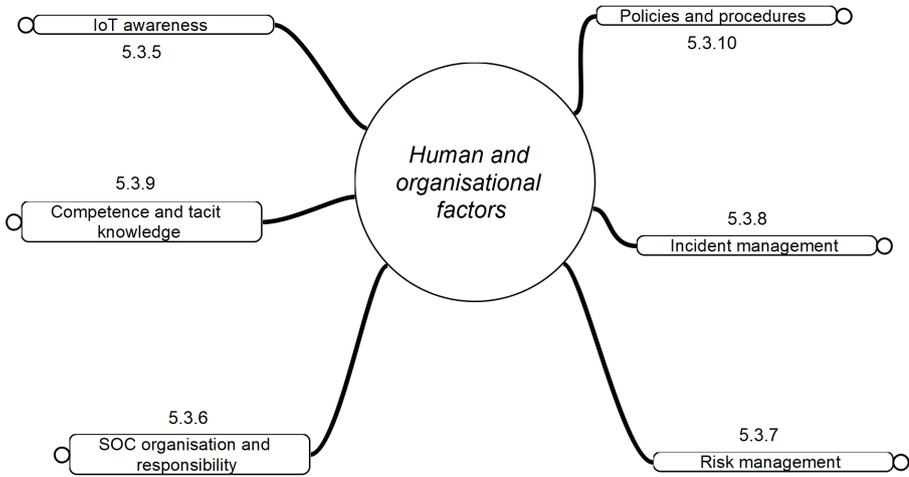


Figure 5.4: A map of human and organisational factor statements for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13 addressing business drivers, monitoring and detection, and SOC from the IoT domain.

5.3.5 IoT awareness

The awareness about IoT- and IIoT devices can be interpreted to be low based on the respondent's answers. According to NSM, the "established security teams do not have such a good relationship

with such IoT devices" (R5). The awareness of IoT is a culture trip in taking back control of what is put into the network infrastructure. However, there are practices that should be followed to make the awareness better and that is to follow guidelines on how to implement a system from the early phases of acquiring a solution to have it in production. According to NSM, this is about following the principles of "plan, implement, operate and improve – getting it into the normal cycle of the SOC" (R5). This makes the SOC work more proactively with a risk-based approach instead of reactive where "a risk migration that IoT can potentially migrate to legacy that does not have such good self-protection and security model thinking" (R5).

5.3.6 SOC organisation and responsibility

SOC has proven to be an important instrument for businesses to measure how systems behave and to detect daily operations and anomalies. A security operation model that fits and aligns with the core business is preferable.

According to NSM the human, technology and organisation perspectives were mentioned of essential importance to balance the activities and it was explicitly mentioned that we "must have human involvement" (R5) when dealing with security incidents in an emerging threat landscape. However, as InfraCERT points out here the link between the organisational operational units' competence and elaboration with IT and OT personnel for situation awareness when an incident must be handled in the organisation.

InfraCERT has mentioned the need for a closer elaboration between IT- and OT operation, and the SecOps teams where "one thing that I think is very lacking is the link between... we call it SOC... IT and OT security people - and those who operate IoT or operate the SCADA system... those who actually control the electricity or heat production" (R6).

5.3.7 Risk management

Balancing the risk and acting based on the system's criticality was mentioned as an important factor when reporting on security KPIs to the upper management level for attention to emergencies. NSM mentioned that security events and incidents should be shared upwards in the organisation and put on the agenda by "get it up to KPI and management level" (R5). Otherwise this "can result in getting a business that is down for a longer period of time..." (R5). According to InfraCERT, it was essential to making risk assessments with mappings to supply chains to govern the business operation by knowing the origin of components and services. Engage the upper leadership and board's responsibility and put security risks on the agenda.

5.3.8 Incident management

In a sourcing model where the business relies on external security services and resources to handle incidents, InfraCERT has shared what they believe the most effective solution would be to have an internal incident response team. This was supported by Equinor if something happens to critical systems there were a high acceptance and attention with a first priority to handle and control the situation impacting the OT system. A SOC's capability to gain quick context of ongoing activities comprised of a series of security events is key to successfully mitigating an incident response.

5.3.9 Competence and tacit knowledge

Every business should assess itself and balance the business risks to what extent a sourcing model could benefit the available human knowledge needed and how much the business will own and handle by itself. Suppliers tend to be in a strong position to provide expert knowledge on products and services and could influence and support the businesses with their operations. According to InfraCERT the competence of mission-critical systems were often found inside the suppliers, and was stated as "naturally because the expertise is found with the suppliers..." (R6) with the risk of the business becoming too dependent on the suppliers.

5.3.10 Policies and procedures

Controlling business needs with governance was mentioned as key when acquiring new systems into an existing system landscape. It would be a success factor for a SecOps team to be able to configure proper security measures and incorporate security monitoring. According to IFE the experience for this remains in the lack of establishing and following procurement processes with security requirements specifications when acquiring new equipment without involving IT or SOC in the onboarding of new devices for life cycle management addressing asset inventory registration, security configuration and patching.

5.3.11 Lesson learned from the industry introducing IoT for security monitoring

We have described some categories of concerns to address for businesses and SOCs. The already mentioned categories are essential to finding and developing a new way of working. One way would be to embrace the agile DevSecOps approach. The next question is **RQ3.1: What does this depend on?**

A future security operation model must take into consideration the speed of the changing threat landscape and the need for quick situation awareness with extensive context from each security event. This puts security analysts under pressure in regard to performance when handling security incidents with a diverse and increased number of different devices. The need for a new operating model relies upon a movement towards an agile SecOps team integrated with a security orchestration, automation and response (SOAR) platform to utilise automation of responses.

The complexity can be divided into two concerns; maintaining legacy and introducing a new system into the system landscape. This can in practice be overwhelming and almost impossible to follow by a SOC. However, there is a need for more automation, "smarter" handling and sense-making of security events to free up resources from SOC analysts and responders. Using an orchestration engine capable to utilise edge computing to contain and mitigate incident sources as close to the source as possible.

Depending on the size of SOC there are often specialised teams called SecOps teams. A SecOps team is a dedicated task force working with security issues by adopting agile development practices for specialising the team with specific knowledge. According to Mnemonic (R3) for operating and maintaining IoT devices in a business context the "complexity is so high and the importance is so great that you have to take this very seriously... this with monitoring... it is very resource-intensive to build this yourself and have control over this..." (R3).

Design principles and standards for developing secure IoT devices and services exist but businesses were slow to adopt and incorporate new practices.

In addition, we have previously found in the state of art and literature review that there exist symptoms of slow adoption of new technology by organisations. However, this is two-folded and were often driven by costs and the return on investment.

5.4 Threats to validity

We have gathered data from six interviews with security professionals in Norway and have focused on not exposing information and statements that could disclose critical infrastructure. This balance could of course impact the result in a way that we miss deeper technical descriptions and practices on how to respond to specific cyber attacks. However, we have an interesting result with 483 statements from different parts of the value chain from device specifications and practices on how things were conducted in regard to operation and security monitoring.

Secrecy is a challenge when discussing security related topics. There is a tendency that the respondents are reluctant to share information as it might constitute a risk. In order to mitigate this we choose to keep the respondents anonymous in the hope that the respondents would feel more comfortable in sharing information. We do not want to expose sensitive information about the organisation or customers. The bias risk of the researcher towards the participants by phrasing questions in different ways for the participant or asking leading questions should not be ruled out but was considered at a minimum. The semi-structured interview with audio recording gave more credibility to the quality of the answers because it does not retain the interpretation by the researcher. The researcher's impression was that they seemed to share more information by being anonymous. Lastly, the majority of the respondents had anonymity as a requirement to participate in the study and for sharing the results.

The process of identifying and highlighting important text from the interviews was done in phase 1 of the thematic analysis. This phase was perhaps the most critical part that could threaten the research validity. The researcher's subjective understanding and knowledge were used to identify text from the transcribed interviews and which text considered from the transcript would be of relevance. Phase 1 threatens validity because it relays mainly on the researcher's own experience and knowledge from working in the field. In addition, there were no team or other researchers to verify the text and how the selection of coding was done. The mean to mitigate this threat the following was performed. Verifying and documenting (1) how this qualitative study was conducted we used the COREQ checklist and answered 32 questions which are available in Appendix D. The (2) iterative process in the method was stringently followed when coding text from the transcripts which helped the researcher maturing and familiarising with the data set.

The reliability relates to the consistency of a measure of how reliable we were able to engage with the participants to provide an answer to the questions. The presentation that was given during the interviews could potentially influence some answers given by the respondents but was considered to be an important part to frame and setting the context. The three main RQs were also presented during the interview with each respondent to provide objectives for the IQs. We should also take into account that we have interviewed only one representative from each SOC.

A general observation from the interviews was that we found and collected less relevant statements to answer the IQs from SIKT (R4). The SIKT (R4) was more unfamiliar with the IoT device's existence in operation concerning monitoring and detection. The quality of the collected data is representative based on the number of SOC that participated and how they responded to each IQ.

Chapter 6

Conclusion and future work

6.1 Conclusion

In this research, we defined four objectives (Chapter 1) in regard to identifying SOC's ability to do security monitoring and handle incidents within a complex system landscape of an increasing number of IoT devices.

We have interviewed security professionals from the Norwegian security community to discover existing practices and gather experiences from people working in the field of operation within IT and OT on the sharp end of handling security incidents. The interviews and the collected material were done in the autumn of 2022. We have discussed the findings and how they answered each RQ using the mappings from the corresponding themes in our data set. The use of thematic analysis on IQs gave us an overview of all sentences with statements provided by the respondents.

The respondents were to some extent not familiarised with the concept of security monitoring of IoT devices. There were fewer experiences shared with handling IoT device security incidents among the respondents and there were more challenges mentioned about IoT than solutions to overcome. This would be related to a long period with legacy devices and a lack of resources and capabilities for IoT devices with options for applying security monitoring parameters. The passive network monitoring method was specially mentioned and used for security monitoring by looking at network traffic and pattern of behaviours with IoT devices.

With fewer experiences mentioned by the different respondents combined with the fact that IoT devices exist in businesses, the onboarding of IoT devices for security monitoring was considered low. The uptake of new IoT technology for incorporation with security monitoring in organisations depends on the maturity of the business and how well the SOC was integrated and aligned with the business from acquiring, implementing, operating and maintaining.

The use of edge computing was considered low on utilisation when addressing new possible detection capabilities closer to the actual physical system. The maturity level of IoT would be considered to still be in its early stages of development and the adoption of use within the industry. However, IoT devices must be taken more seriously when set into production with respect to gaining control of what is put into the corporate network that could be introduced as a risk.

This qualitative research has increased the knowledge about IoT devices and their capabilities in security monitoring experienced by the different SOCs in Norway. This research has also identified different techniques and security monitoring parameters currently used for anomaly detection for IoT devices.

We have highlighted some problem areas for further exploration; the adoption of standards in the development of IoT devices, and integrating the SOC into the practical DevSecOps for continuous improvement of lifecycle management for security detection.

With the recent development of IoT guidelines and standards for developing and managing safe and secure IoT and OT devices, the IoT Security Foundation (IoTSF, 2023) has mentioned the use of the Software Bill of Materials (SBOM). The SBOM describes software components and their relations which enable IoT/OT vendors to generate and share SBOMs for automating the scanning for known vulnerabilities. According to IoT Security Foundation this would provide a common basis for "how IoT/OT vendors should generate and share SBOMs, and how everyone in the IoT/OT supply chain should use SBOMs to effectively reduce cyber risks for IoT/OT operators" (IoTSF, 2023, p. 8).

We must start adopting IoT standards in everyday work, practice and implement security monitoring for øholistic situation awareness, and act more proactively by addressing technical IoT security capabilities and requirements. The SOCs should incorporate security monitoring of IoT devices into their regular monitoring solutions.

6.2 Future work

The development of competencies and skills will always be beneficial for a broader understanding of the challenges of managing vulnerable devices. A SOC should adopt the DevOps agile method to train dedicated SecOps teams in the use of tools to speed up security development by building competencies and sharing experiences from real-world cases. In addition, the suppliers must take a bigger responsibility to develop sustainable products with lifecycle device management and adopt IoT standards and frameworks for secure product development.

Bibliography

- ABB. (2023). Ripple20 Advisory impact on Distribution Automation products. Retrieved April 5, 2023, from <https://search.abb.com/library/Download.aspx?DocumentID=2NGA000473&LanguageCode=en&DocumentPartId=&Action=Launch>
- Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2021). A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things [Section: 4004]. *IEEE Internet of Things Journal*, 8(6), 4004–4022. <https://doi.org/10.1109/jiot.2020.3015432>
- Analytics, I. (2021). State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. Retrieved February 23, 2022, from <https://iot-analytics.com/number-connected-iot-devices/>
- AWS, A. (2022). What is DevOps? - Amazon Web Services (AWS). Retrieved September 18, 2022, from <https://aws.amazon.com/devops/what-is-devops/>
- Basir, R., Qaisar, S., Ali, M., Aldwairi, M., Ashraf, M. I., Mahmood, A., & Gidlund, M. (2019). Fog Computing Enabling Industrial Internet of Things: State-of-the-Art and Research Challenges [Edition: 20191105]. *Sensors (Basel)*, 19(21). <https://doi.org/10.3390/s19214807>
- Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems [Section: 3496]. *IEEE Communications Surveys & Tutorials*, 20(4), 3496–3509. <https://doi.org/10.1109/comst.2018.2844742>
- Bertino, E. (2019). IoT Security A Comprehensive Life Cycle Framework, 196–203. <https://doi.org/10.1109/cic48465.2019.00033>
- Boyd, J. A. (2018). A Discourse on Winning and Losing. *Air University Press*, 400. https://www.coljohnboyd.com/static/documents/2018-03__Boyd_John_R__edited_Hammond_Grant_T__A_Discourse_on_Winning_and_Losing.pdf
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology [Publisher: Routledge _eprint: <https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp0630a>]. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? [Publisher: Routledge _eprint: <https://doi.org/10.1080/14780887.2020.1769238>]. *Qualitative Research in Psychology*, 18(3), 328–352. <https://doi.org/10.1080/14780887.2020.1769238>
- Callum, C. (2022). DevSecOps Brings Payoffs through Security by Design. Retrieved September 18, 2022, from <https://www.iiotworldtoday.com/2021/08/02/devsecops-brings-payoffs-through-security-by-design/>
- Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2019). Toward the automation of threat modeling and risk assessment in IoT systems [Section: 100056]. *Internet of Things*, 7. <https://doi.org/10.1016/j.jiot.2019.100056>

- Casola, V., De Benedictis, A., Riccio, A., Rivera, D., Mallouli, W., & de Oca, E. M. (2019). A security monitoring system for internet of things [Section: 100080]. *Internet of Things*, 7. <https://doi.org/10.1016/j.iot.2019.100080>
- Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques [Section: 2671]. *IEEE Communications Surveys & Tutorials*, 21(3), 2671–2701. <https://doi.org/10.1109/comst.2019.2896380>
- CISCO. (2023). Cisco IOS Netflow Data Sheet. Retrieved May 7, 2023, from https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/product_data_sheet0900aecd80173f71.html
- Colelli, R., Panzieri, S., & Pascucci, F. (2019). Securing connection between IT and OT: The Fog Intrusion Detection System prospective. <https://doi.org/10.1109/metroi4.2019.8792884>
- Collins. (2023). Challenge definition and meaning | Collins English Dictionary. Retrieved February 7, 2023, from <https://www.collinsdictionary.com/dictionary/english/challenge>
- Crowley, C., & Pescatore, J. (2018). *The Definition of SOC-cess?* (Survey). SANS Institute. Retrieved February 5, 2023, from <https://sansorg.egnyte.com/dl/WW7a2XzVsz>
- Dimitrov, W., & Syarova, S. (2019). Analysis of the Functionalities of a Shared ICS Security Operations Center, 1–6. <https://doi.org/10.1109/BdKCSE48644.2019.9010607>
- Dun, Y. T., Ab Razak, M. F., Zolkiplib, M. F., Bee, T. F., & Firdaus, A. (2021). Grasp on next generation security operation centre NGSOC): Comparative study. *International Journal of Nonlinear Analysis and Applications*, 12(2). <https://doi.org/10.22075/ijnaa.2021.5145>
- E. Storm, B., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and Philosophy. Retrieved May 7, 2023, from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- ENISA. (2015). Supply Chain Integrity. Retrieved May 19, 2023, from <https://www.enisa.europa.eu/publications/sci-2015>
- ENISA. (2021). Threat Landscape for Supply Chain Attacks. Retrieved May 19, 2023, from <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>
- Equinor, N. (2023). Norway. Retrieved January 3, 2023, from <https://www.equinor.com/where-we-are/norway>
- European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. Publications Office. Retrieved May 9, 2023, from <https://data.europa.eu/doi/10.2824/764318>
- Faid, A., Sadik, M., & Sabir, E. (2022). An Agile AI and IoT-Augmented Smart Farming: A Cost-Effective Cognitive Weather Station [Number: 1 Publisher: Multidisciplinary Digital Publishing Institute]. *Agriculture*, 12(1), 35. <https://doi.org/10.3390/agriculture12010035>
- Ferencz, K., Domokos, J., & Kovacs, L. (2021). Review of Industry 4.0 Security Challenges, 245–248. <https://doi.org/10.1109/saci51354.2021.9465613>
- FIRST. (2023). Common Vulnerability Scoring System SIG. Retrieved March 4, 2023, from <https://www.first.org/cvss>
- Furdek, M., Natalino, C., Di Giglio, A., & Schiano, M. (2020). Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats [Invited] [Section: A144]. *Journal of Optical Communications and Networking*, 13(2). <https://doi.org/10.1364/jocn.402884>
- Gartner. (2023). Definition of Security Information And Event Management (SIEM) - Gartner Information Technology Glossary. Retrieved May 7, 2023, from <https://www.gartner.com/>

[en/information-technology/glossary/security-information-and-event-management-siem](#)

- George, T. (2021). Exploratory Research | Definition, Guide, & Examples. Retrieved January 11, 2023, from <https://www.scribbr.com/methodology/exploratory-research/>
- Goodall, J. R., Ragan, E. D., Steed, C. A., Reed, J. W., Richardson, G. D., Huffer, K. M. T., Bridges, R. A., & Laska, J. A. (2018). Situ: Identifying and Explaining Suspicious Behavior in Networks [Edition: 20180820]. *IEEE Trans Vis Comput Graph*. <https://doi.org/10.1109/TVCG.2018.2865029>
- Hadar, E., & Hassanzadeh, A. (2019). Big Data Analytics on Cyber Attack Graphs for Prioritizing Agile Security Requirements, 330–339. <https://doi.org/10.1109/re.2019.00042>
- Hamad, S. A., Sheng, Q. Z., Zhang, W. E., & Nepal, S. (2020). Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies [Section: 1372]. *IEEE Communications Surveys & Tutorials*, 22(2), 1372–1391. <https://doi.org/10.1109/comst.2020.2976075>
- Hassanzadeh, A., & Burkett, R. (2018). SAMIIT: Spiral Attack Model in IIoT Mapping Security Alerts to Attack Life Cycle Phases. <https://doi.org/10.14236/ewic/ICS2018.2>
- Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence Based Nursing*, 18(3), 66–67. <https://doi.org/10.1136/eb-2015-102129>
- Henshaw, M., Dahmann, J., & Lawson, B. (2022). Systems of Systems (SoS) - SEBoK. Retrieved September 18, 2022, from [https://www.sebokwiki.org/wiki/Systems_of_Systems_\(SoS\)](https://www.sebokwiki.org/wiki/Systems_of_Systems_(SoS))
- Hewlett Packard, H. (2022). What is Security Monitoring? | Glossary. Retrieved September 19, 2022, from https://www.hpe.com/emea_europe/en/what-is/security-monitoring.html
- Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the Energy Sector [Section: 494]. *Energies*, 13(2). <https://doi.org/10.3390/en13020494>
- IFE. (2023). About IFE. Retrieved January 3, 2023, from <https://ife.no/en/about-ife/>
- IoTSF. (2023). *Software Bills of Materials for IoT and OT devices* (tech. rep.). IoT Security Foundation. Retrieved March 5, 2023, from <https://www.iotsecurityfoundation.org/wp-content/uploads/2023/02/RELEASE-2022-02-19-IoTSF-SBOM-whitepaper-v1-1-0.pdf>
- Jackson Higgins, K. (2021). Lights Out: Cyberattacks Shut Down Building Automation Systems [Section: attacks-breaches]. Retrieved June 6, 2023, from <https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems>
- JSOF. (2020). Ripple20. Retrieved January 22, 2023, from <https://www.jsf-tech.com/disclosures/ripple20/>
- Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide [eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/jan.13031>]. *Journal of Advanced Nursing*, 72(12), 2954–2965. <https://doi.org/10.1111/jan.13031>
- Kent, K., & Souppaya, M. P. (2006). *Guide to computer security log management* (tech. rep. NIST SP 800-92) [Edition: 0]. National Institute of Standards and Technology. Gaithersburg, MD. <https://doi.org/10.6028/NIST.SP.800-92>
- KEV, C. (2023). Known Exploited Vulnerabilities Catalog | CISA. Retrieved April 5, 2023, from <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges [Section: 106522]. *Computers & Electrical Engineering*, 81. <https://doi.org/10.1016/j.compeleceng.2019.106522>
- KraftCERT. (2023). InfraCERT. Retrieved January 3, 2023, from <https://www.kraftcert.no/en/#om>

- Maguire, M., & Delahunt, B. (2017). *Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars*. 8(3).
- Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of Threats to the Internet of Things [Section: 1636]. *IEEE Communications Surveys & Tutorials*, 21(2), 1636–1675. <https://doi.org/10.1109/comst.2018.2874978>
- Mathezer, S. (2021). Introduction to ICS Security Part 2 | SANS Institute. Retrieved February 26, 2023, from <https://www.sans.org/blog/introduction-to-ics-security-part-2/>
- Miessler, D. (2021). The Difference Between Events, Alerts, and Incidents. Retrieved March 2, 2023, from <https://danielmiessler.com/study/event-alert-incident/>
- MITRE. (2023a). MITRE ATT&CK®. Retrieved May 7, 2023, from <https://attack.mitre.org/#>
- MITRE. (2023b). Replication Through Removable Media, Technique T1091 - Enterprise | MITRE ATT&CK®. Retrieved May 7, 2023, from <https://attack.mitre.org/techniques/T1091/>
- MITRE. (2023c). Wireless Compromise, Technique T0860 - ICS | MITRE ATT&CK®. Retrieved May 7, 2023, from <https://attack.mitre.org/techniques/T0860/>
- Mnemonic. (2023). Who is mnemonic? Retrieved January 3, 2023, from <http://www.mnemonic.io/company/>
- Nathans, D. (2014). *Designing and Building Security Operations Center*. Syngress.
- NCSC, U. (2023). Preventing Lateral Movement. Retrieved April 24, 2023, from <https://www.ncsc.gov.uk/guidance/preventing-lateral-movement>
- Ni, J., Lin, X., & Shen, X. S. (2019). Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives [Section: 50]. *IEEE Network*, 33(2), 50–57. <https://doi.org/10.1109/mnet.2019.1800229>
- NIST. (2022). Information security continuous monitoring (ISCM) - Glossary | CSRC. Retrieved September 19, 2022, from https://csrc.nist.gov/glossary/term/information_security_continuous_monitoring
- NIST. (2023). Asset - Glossary | CSRC. Retrieved February 11, 2023, from <https://csrc.nist.gov/glossary/term/asset>
- NIST, C. C. (2022). Internet of Things (IoT) - Glossary | CSRC. Retrieved February 19, 2022, from https://csrc.nist.gov/glossary/term/internet_of_things_iiot
- NIST, C. C. (2023). Tactics, techniques, and procedures (TTP) - Glossary | CSRC. Retrieved May 7, 2023, from https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures
- NSM. (2020). Norwegian National Cyber Security Centre (NCSC) - Nasjonal sikkerhetsmyndighet. Retrieved January 3, 2023, from <https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/>
- OpenDataWatch. (2018). The Data Value Chain: Moving from Production to Impact [Section: Publications]. Retrieved March 5, 2023, from <https://opendatawatch.com/publications/the-data-value-chain-moving-from-production-to-impact/>
- Peiris, C., Pillai, B., & Kudrati, A. (2021). *Threat Hunting in the Cloud*. John Wiley & Sons. https://books.google.no/books?id=RHpAEAAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0
- Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). Survey on Multi-Access Edge Computing for Internet of Things Realization [Section: 2961]. *IEEE Communications Surveys & Tutorials*, 20(4), 2961–2991. <https://doi.org/10.1109/comst.2018.2849509>
- Qiu, Q., Wang, D., Du, X., Yu, S., Liu, S., & Zhao, B. (2021). Security Standards and Measures for Massive IoT in the 5G Era. *Mobile Networks and Applications*. <https://doi.org/10.1007/s11036-021-01841-2>

- Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. (2020). Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges [Section: 2462]. *IEEE Communications Surveys & Tutorials*, 22(4), 2462–2488. <https://doi.org/10.1109/comst.2020.3009103>
- Rajamäki, A. (2021). *Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center* (Master's thesis). Jamk University of Applied Sciences.
- Rapuzzi, R., & Repetto, M. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model [Section: 235]. *Future Generation Computer Systems*, 85, 235–249. <https://doi.org/10.1016/j.future.2018.04.007>
- Ray, P. P., Dash, D., & De, D. (2019). Edge computing for Internet of Things: A survey, e-healthcare case study and future direction [Section: 1]. *Journal of Network and Computer Applications*, 140, 1–22. <https://doi.org/10.1016/j.jnca.2019.05.005>
- Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains [Section: 251]. *Future Generation Computer Systems*, 115, 251–266. <https://doi.org/10.1016/j.future.2020.08.044>
- Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges [Section: 680]. *Future Generation Computer Systems*, 78, 680–698. <https://doi.org/10.1016/j.future.2016.11.009>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (tech. rep.). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- Santos, D. d. (2020). Identifying and Protecting Devices Vulnerable to Ripple20. Retrieved April 2, 2023, from <https://www.forescout.com/blog/identifying-and-protecting-devices-vulnerable-to-ripple20/>
- Security, M. (2022). Microsoft Security DevOps. Retrieved September 18, 2022, from <https://www.microsoft.com/en-us/securityengineering/devsecops>
- SIKT. (2023). Cybersikkerhetscenter for forskning og utdanning | Sikt. Retrieved January 3, 2023, from <https://sikt.no/en/tjenester/cybersikkerhetscenter-forskning-og-utdanning>
- Simon, B. (2021). Complete Guide to the PPT Framework | Smartsheet. Retrieved February 5, 2023, from <https://www.smartsheet.com/content/people-process-technology>
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022). *Guide to Operational Technology (OT) Security: Initial Public Draft* (preprint). <https://doi.org/10.6028/NIST.SP.800-82r3.ipd>
- Tagarev, T., & Sharkov, G. (2019). Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems, 8–18. <https://doi.org/10.1145/3345252.3345255>
- Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*, 19(6), 349–357. <https://doi.org/10.1093/intqhc/mzm042>
- Urooj, U., Al-rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions [Number: 1 Publisher: Multidisciplinary Digital Publishing Institute]. *Applied Sciences*, 12(1), 172. <https://doi.org/10.3390/app12010172>
- Vavra, C. (2021). System integrator competencies in the age of IT/OT convergence. Retrieved February 26, 2023, from <https://www.controleng.com/articles/system-integrator-competencies-in-the-age-of-it-ot-convergence/>

- Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges [Section: 227756]. *IEEE Access*, 8, 227756–227779. <https://doi.org/10.1109/access.2020.3045514>
- Wallin, E. (2022). Building Management Systems for Smart Buildings. Retrieved May 19, 2023, from <https://proptechos.com/building-management-systems/>
- Weissman, D., & Jayasumana, A. (2020). Integrating IoT Monitoring for Security Operation Center, 1–6. <https://doi.org/10.1109/GIOTS49054.2020.9119680>
- Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering, 1–10. <https://doi.org/10.1145/2601248.2601268>

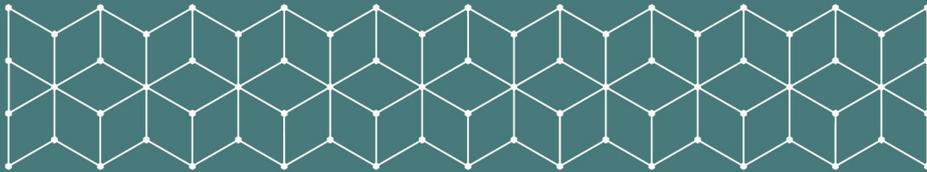
Appendix A

Interview guide

Security Operation Centers and IoT How should SOCs monitor IoT assets for effective detection and response?

Semi-structured Interview

Per-Arne Jørgensen
Master in Applied Computer Science
2022



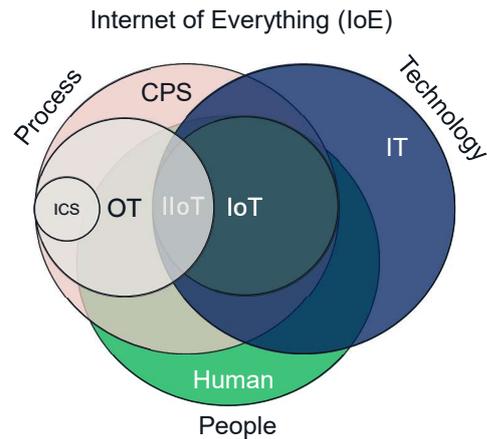
04.02.2023 1

Formål og samtykke

- Få vite mer om hvordan IoT-enheter og systemer typisk håndteres av SOC (Security Operation Centre) / CERTs (Computer Emergency Response Team) / IRT (Incident Response Team) og hvilke utfordringer som eksisterer i dag.
- Samtykke
 - Du kan når som helst trekke samtykket tilbake uten å oppgi noen grunn.
 - Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil bidra eller senere velger å trekke deg.
 - Du kan også velge å ikke svare på spørsmålene
 - Utsagn, personlige meninger, problemstillinger, etc. som kommer frem under intervjuet vil bli anonymisert

Introduction – SOC & IoT

- The future role of SOC-function and the emerging adoptions of connected things.
 - Different SOC operation models
- IT/OT convergence
 - Industry Internet of Things (IIoT)
 - Internet of Everything (IoE)
 - Cyber Physical Systems (CPS)
 - PLC
 - Industrial Control Systems (ICS) / SCADA
 - Edge Computing
 - Embedded system (IoT device, firmware etc)
 - Raspberry Pi
 - IoT Gateways
 - Protocol gateways
 - Self-contained microcontroller
 - Arduino
 - ESP32 / ESP8266
- Process oriented
- Sensor
 - Temperature/Humidity
- Actuator (control)
 - Switch, Pump, Servo etc.



[Cyber-Physical Systems and Internet of Things \(nist.gov\)](https://www.nist.gov/cyber-physical-systems-and-internet-of-things)

SOC sin rolle I fremtiden

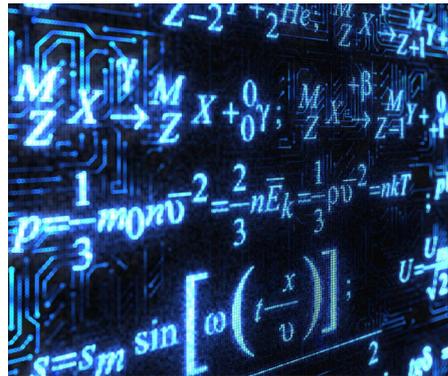
Cisco defined Internet of Everything (IoE) as the networked connection of people, process, data, and things.

The benefit of IoE is derived from the compound impact of connecting people, process, data, and things, and the value this increased connectedness creates as “everything” comes online.

[ioe-value-index-faq.pdf \(cisco.com\)](https://www.cisco.com/ie-value-index-faq.pdf)

Problem statement

- How should SOCs monitor IoT assets for effective detection and response?



Research Questions

RQ1: What are the challenges in security monitoring, maintaining and operating IoT devices?

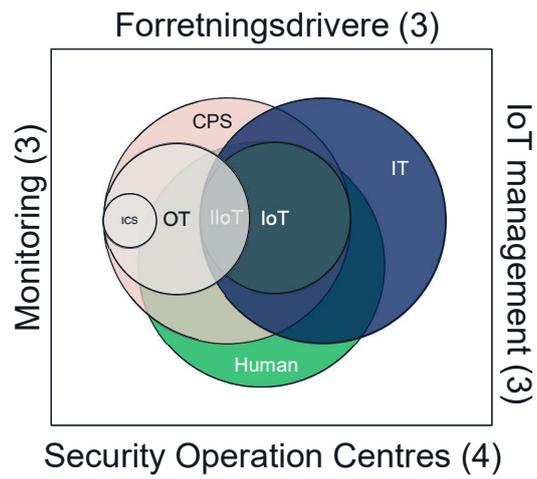
- *RQ1.1: What is the challenge seen from the SOC's perspective on monitoring IoT devices?*
- *RQ1.2: What is the state-of-art for monitoring IoT devices?*

RQ2: What type of information is collected from IoT devices to detect anomalies and what data does this rely on?

- *RQ2.1: What type of remediation methods is used to mitigate IoT security events/alerts and incidents?*

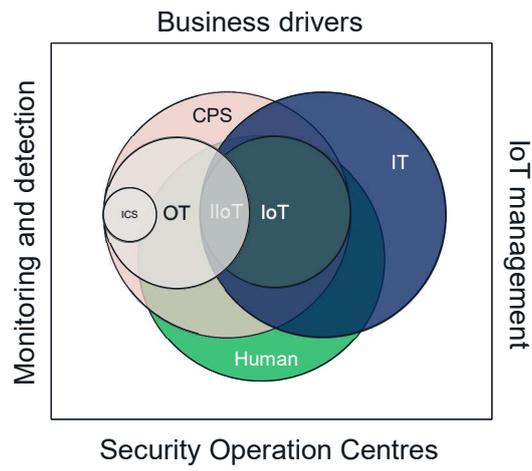
RQ3: How should a SOC operate and work in the future to adapt to monitor the increasing number of IoT devices?

- *RQ3.1: What does this depend on?*



13 spørsmål

Hvilket perspektiv eller kontekst ønsker du å svare ut i fra?



Hvilket perspektiv eller kontekst ønsker du å svare ut i fra?

Spørsmål 1 (Forretningsdrivere)

- › I hvilken grad vil du si at virksomheter(en) benytter seg av eller har IoT-enheter?



This Photo by Unknown Author is licensed under CC BY-SA-NC

04.02.2023 8

Eksisterer det? Er det i drift?

Hvordan definerer du IoT hva betyr det for deg?

Er virksomhetene klar over at slike IoT enheter eksisterer?

Hva er dine erfaringer med bruk av IoT/Indstri-IoT/OT?

Er IoT en del av det du jobber med til daglig?

Spørsmål 2 (Forretningsdrivere)



- Hvor viktig (kritisk eller avhengig) vil du si at IoT er for virksomheten?

04.02.2023 9

Har du noen eksempler på et typiske IoT - use case (brukstilfeller) eller system?

Har du noen eksempler på hva brukes IoT til i bedriften?

Hvordan er IoT-enheter registrert?

Spørsmål 3 (Forretningsdrivere)

- › Hvordan tror du at IoT har eller vil påvirke bedrifts- eller virksomhetsnettverket?



04.02.2023 10

Er bruken av IoT med på å drive/påvirke virksomhetsnettverket?

Hvordan tenker du det bør være i framtiden?
På hvilken måte?

Hva tror du dette avhenger av?

Modenhet?

Arkitektur?

Standarder?

Teknologier?

Annet?

Spørsmål 5 (IoT)

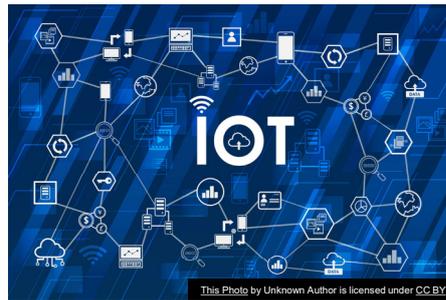


- Hva vil du si er utfordringene med ulike IoT-systemer i dag?

Har du noen eksempler på utfordringer med IoT?

Spørsmål 6 (IoT)

- › Hvilken type sikkerhetsbarrierer/mekanismer er nødvendige for å beskytte slike IoT-enheter?



04.02.2023 13

Hva tenker du gir best beskyttelse for slike enheter?

Benyttes det noen form for kantløsninger (edge) foran IoT-enhetene?

Er det implementert eller brukt IPv6 for IoT-nettverket?

Hvilken type IoT-tilkobling er mest brukt - kablet eller trådløs, eller begge deler?

Spørsmål 7 (Monitorering)

- › Hvordan bør IoT-enheter vedlikeholdes og overvåkes?



04.02.2023 14

Hvor ofte tenker du sikkerhetsoppdateringer bør utføres?

Har du noen eksempler på hvordan dette kan utføres mest effektivt?

Hvilken type rolle (rolle/enhet) er ansvarlig for å vedlikeholde IoT-enheter?

Spørsmål 8 (Monitorering)

- Hvordan logger og rapporterer IoT-enheter?



04.02.2023 15

Benyttes det noen for Security information and event management (SIEM) løsning?

Hvilken type parametere overvåkes vanligvis på en IoT-enhet?

Hvorfor benyttes akkurat disse parameterne?

Er det overvåkingsparametere du ønsker å ha eller mangler i dag?

Spørsmål 10 (SOC)

- › Hvordan tenker du IoT-enheter bør introduseres for et SOC-team for sikkerhets monitorering?



04.02.2023 17

Hvordan er SOC-teamets forhold til IoT-enheter? Har SOC et forhold til slike enheter?

Hvordan bør IoT-enheter ombordes eller introdusere for monitorering?

Spørsmål 11 (SOC)



- Hvordan tenker du SOC bør organiseres for en optimal monitorering av IoT-enheter?

Er det spesialiserte IT/OT eller IoT sikkerhetsteam for håndtering av IoT-enheter/systemer?

Spørsmål 12 (SOC)

- På hvilken måte er organisering av SOC påvirket av forretningsmålene?



04.02.2023 19

Hvordan gir SOC bevis for et oppdatert risikobilde over IoT-enheter?

Spørsmål 13 (SOC)

- › Hvilken type SOC-driftsmodell bør benyttes for IoT?



04.02.2023 20

Inhouse?

Outsourced? Hybrid?

Vil du si at leverandørene driver IoT-utviklingen?

Hvordan får man kontroll på IoT enheter?

Hvordan vil du beskrive den optimale integrasjonen av IoT i en SOC?



Tusen takk for din tid og bidrag!

Per-Arne Jørgensen

04.02.2023 21

Appendix B

Interview and consent formular

Vil du bidra til masterprosjektet

“Security Operations Center (SOC) and Internet-of-Things (IoT) - Introducing IoT monitoring”?

Dette er et spørsmål til deg om å delta i min masteroppgave hvor formålet er å utforske hvordan Security Operations Centres bør overvåke Internet-of-Things (IoT)-enheter og ressurser for effektiv deteksjon og respons. Vi tror at dine meninger og kompetanse vil være av verdifull informasjon for vår forskning.

Masterarbeidet ønsker å undersøke hvordan IoT-enheter og systemer definerer sine grensesnitt for en mest mulig effektiv overvåking fra tidlig fase innen deteksjon til en hendelseshåndteringsprosess med typiske responsstrategier ved cyber angrep.

I dette skrevet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med intervju er å gi en bedre oversikt og innsikt i hvordan IoT-enheter og systemer håndteres av sikkerhetsteam, internt i en organisasjon eller erfaringer/meninger fra personer med kompetanse på området. Informasjonen som samles inn vil kunne justere forskningens mål og spørsmål basert på resultatet.

Forskningsprosjektet er en del av en masteroppgave i *Cyber Physical Systems* ved **Høgskolen i Østfold**. Intervjuspørsmålene inngår i en masteroppgave og er utformet slik at intervjuobjektene kan gi sin mening om temaet. Formålet med informasjons innhenting er å få vite mer om hvordan IoT-enheter og systemer typisk håndteres av SOC (Security Operation Centre) / CERTs (Computer Emergency Response Team) / IRT (Incident Reponse Team) og hvilke utfordringer som eksisterer i dag.

Hvem er ansvarlig for forskningsprosjektet?

Høgskolen i Østfold er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Utvalget er basert på studentens tidligere relasjoner innen sikkerhetsmiljøet og kjennskap til kandidatens erfaringer innen temaet. Utvalget er gjort basert på seks (6) henvendelser til aktuelle kandidater om deltagelse hvor de også har en relasjon til SOC'er/CERT'er i Norge.

Hva innebærer det for deg å delta?

Hvis du velger å bidra i prosjektet, innebærer det at du samtykker til å bli intervjuet. Jeg søker kun dine egne meninger og erfaring på temaet/området. Navnet på organisasjonen (SOC/CERT) du tilhører blir brukt til å kategorisere svar. Det vil ta deg ca 45-60 minutter.

Intervjuet vil gjennomføres fysisk og/eller digitalt på Høgskolen i Østfolds Microsoft 365 Teams tjeneste.

Spørsmålene stilles til deg gjennom en Powerpoint presentasjon, hvor jeg først tar en rask introduksjon og deretter tar lydopptak av intervjuet og tar notater.

Intervjuet vil gi innspill og informasjon for å teste en hypotese eller demonstrere en metode. Presentasjonen inneholder spørsmål om bruk av IoT-enheter i organisasjoner, utfordringer og typiske sikkerhetsmekanismer i bruk, samt hvordan IoT-enheter bør vedlikeholdes og overvåkes fra en SOC.

Det er frivillig å bidra

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

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

Det er kun master studenten og veilederen som vil ha tilgang til rå-materialet som lydopptaket og innsamlet data og notater. Utsagn, personlige meninger, problemstillinger, etc. som kommer frem under intervjuet vil bli anonymisert og benyttet i oppgaven.

Microsoft Office 365 til Høgskolen i Østfold vil bli brukt som lagringsområde for notater og innsamlet data. Nettskjema sin Diktafon app vil bli brukt til lydopptaket og lagres i Nettskjema på godkjent lagringstjeneste i Norge.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes når oppgaven blir godkjent i løpet av 2023.

Lydopptaket blir slettet etter prosjektslutt. Det er kun anonymiserte opplysninger som kan bli benyttet i masteroppgaven.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Høgskolen i Østfold har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

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

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

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

- Høgskolen i Østfold ved *Øystein Haugen*, Professor, oystein.haugen@hiof.no, kontaktes på telefon: 913 90 914
- Vårt personvernombud: *Julie Dessen*, personvern@hiof.no, kontaktes på telefon: 950 61 930

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

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Øystein Haugen
Prosjektansvarlig
Professor

Per-Arne Jørgensen
Master student

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "*Security Operations Center (SOC) and Internet-of-Things (IoT) - Introducing IoT monitoring*" og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å gjennomføre intervjuet
- at det gjøres lydopptak av meg som lagres elektronisk
- at notater og innsamlet informasjon lagres elektronisk
- at informasjon jeg bringer fram kan brukes i prosjektoppgaven
- at personopplysninger om meg slettes etter prosjektslutt innen 31.12.2023.

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

(Signert av prosjektdeltaker, dato)

Appendix C

Qualitative Data Analysis

Qualitative data analysis		Business drivers						IoT management						Monitoring and detection						Security Operation Centres							
		IQ1		IQ2		IQ3		IQ4		IQ5		IQ6		IQ7		IQ8		IQ9		IQ10		IQ11		IQ12		IQ13	
		To what extent would you say that functionality will or has IoT devices?		How important (critical or dependent) would you say IoT is to your business?		How do you think IoT will or will not impact your enterprise or enterprise network?		Do you anticipate (critical or dependent) IoT and OT technologies (OT devices in how you handle and operate these devices/systems)?		What would you say are the challenges with different IoT system tools?		What type of security barriers/techniques are necessary to protect each IoT device?		How do IoT devices impact and support?		A major computing or control gateway for monitoring IoT devices containing that is used today?		How do you think IoT devices should be monitored or a security monitoring IoT team?		How do you think SOC should be organized for optimal monitoring of IoT devices?		In what way is the organization of the SOC influencing the business objectives?		What type of SOC operating model should be used for IoT?			
Research Question (RQ)	Themes / Topics	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers	Number of SDCs answered	Number of answers
RQ1	Challenges	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Metrics, risks and alerts	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
RQ2	IoT and OT infrastructures	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	Threats and organizational challenges	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
RQ3	Threats and vulnerabilities	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	Threats and vulnerabilities	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

Researchability score (functionality of SDC answered)	5
Number of interview participants	5



Appendix D

COREQ checklist

Consolidated criteria for reporting qualitative studies (COREQ): 32-item checklist

Allison Tong, Peter Sainsbury, Jonathan Craig, Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups, *International Journal for Quality in Health Care*, Volume 19, Issue 6, December 2007, Pages 349–357,

No	Item	Guide questions/description	Answer
Domain 1: Research team and reflexivity			
<i>Personal Characteristics</i>			
1	Interviewer/facilitator	Which author/s conducted the interview or focus group?	One researcher, the master student
2	Credentials	What were the researcher's credentials? E.g. PhD, MD	Master student, part-time
3	Occupation	What was their occupation at the time of the study?	Head of Security Operation Center at Institute for Energy Technology
4	Gender	Was the researcher male or female?	Male
5	Experience and training	What experience or training did the researcher have?	The student have done one semi-structured interview earlier in an Interaction design course. From work experience the student have done several job interviews as a department head.
<i>Relationship with participants</i>			
6	Relationship established	Was a relationship established prior to study commencement?	Yes, with 2 of 6 participant a relationship was established prior to study start. The relationship were professional based on the knowledge of the participants competence and company affiliation.
7	Participant knowledge of the interviewer	What did the participants know about the researcher? e.g. personal goals, reasons for doing the research	The participants did not know about the researchers. The reason for doing the research were presented in a consent form prior to participation in the study.
8	Interviewer characteristics	What characteristics were reported about the interviewer/facilitator? e.g. Bias, assumptions, reasons and interests in the research topic	A short presentation about the research problem and research questions were presented for each participant, before presenting the interview questions.
Domain 2: Study design			
<i>Theoretical framework</i>			
9	Methodological orientation and Theory	What methodological orientation was stated to underpin the study?	Thematic analysis (Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. <i>Qualitative Research in Psychology</i> , 3(2), 77–101. https://doi.org/10.1191/1478088706qp0630a)
<i>Participant selection</i>			
10	Sampling	How were participants selected? e.g. purposive, convenience, consecutive, snowball	The participants were selected based on the purposive mean and the researchers knowledge from working in the Norwegian cybersecurity community.
11	Method of approach	How were participants approached? e.g. face-to-face, telephone, mail, email	All the participants were initially approached by an email asking about their interest to participate in a research study addressing SOC and IoT. A follow-up phone call were conducted to schedule date and time.
12	Sample size	How many participants were in the study?	6 participants
13	Non-participation	How many people refused to participate or dropped out? Reasons?	1 participant did not reply to the initial email and with no response from the followup phone call.
14	Setting of data collection	Where was the data collected? e.g. home, clinic, workplace	The interviews were conducted during working hours in a dedicated office workplace. The interviews were done face-to-face using the video-conference tool MS Teams.
15	Presence of non-participants	Was anyone else present besides the participants and researchers?	No, only the researcher (master student)
16	Description of sample	What are the important characteristics of the sample?	Semi structured interview about SOC's capabilities to monitor and handle the increasing number of IoT devices.
Data collection			

17	Interview guide	Were questions, prompts, guides provided by the authors? Was it pilot tested?	13 interview questions were presented in a Powerpoint presentation, one slide for each questions. The interview guide was not pilot tested in beforehand.
18	Repeat interviews	Were repeat interviews carried out? If yes, how many?	No, no repeating interviews were conducted.
19	Audio/visual recording	Did the research use audio or visual recording to collect the data?	Yes, the data collection from the interviews were audio recorded.
20	Field notes	Were field notes made during and/or after the interview or focus group?	No field notes were made during or after the interviews.
21	Duration	What was the duration of the interviews or focus group?	45-50 minutes
22	Data saturation	Was data saturation discussed?	No
23	Transcripts returned	Were transcripts returned to participants for comment and/or correction?	No
Domain 3: Analysis and findings			
Data analysis			
24	Number of data coders	How many data coders coded the data?	Only one, the researching master student
25	Description of the coding tree	Did authors provide a description of the coding tree?	In the QDA sheet the phase 1 to 5 of thematic analysis were presented with initial themes and coding. In addition, 'mind maps' were used to represent the relationship between themes and statements.
26	Derivation of themes	Were themes identified in advance or derived from the data?	Partly in advanced and refined during analysis based on Braun & Clarke's method for thematic analysis.
27	Software	What software, if applicable, was used to manage the data?	Diktafon App for recording the interviews and manual transcription using MS Word and MS Excel for thematic analysis.
28	Participant checking	Did participants provide feedback on the findings?	The participant did not provide feedback on the findings.
Reporting			
29	Quotations presented	Were participant quotations presented to illustrate the themes / findings? Was each quotation identified? e.g. participant number	Yes, each quotations were numbered and anonymised and mapped to a theme.
30	Data and findings consistent	Was there consistency between the data presented and the findings?	Yes, there was consintence between data and findings, however the finding were based on the analysis and perception of the data from one researcher.
31	Clarity of major themes	Were major themes clearly presented in the findings?	Two of the major themes were "challenges" with 118 statements and "IT and OT infrastrcuture" with 104 statements.
32	Clarity of minor themes	Is there a description of diverse cases or discussion of minor themes?	The two minor themes were "assets" with 18 statements and "devices" with 23 statements.

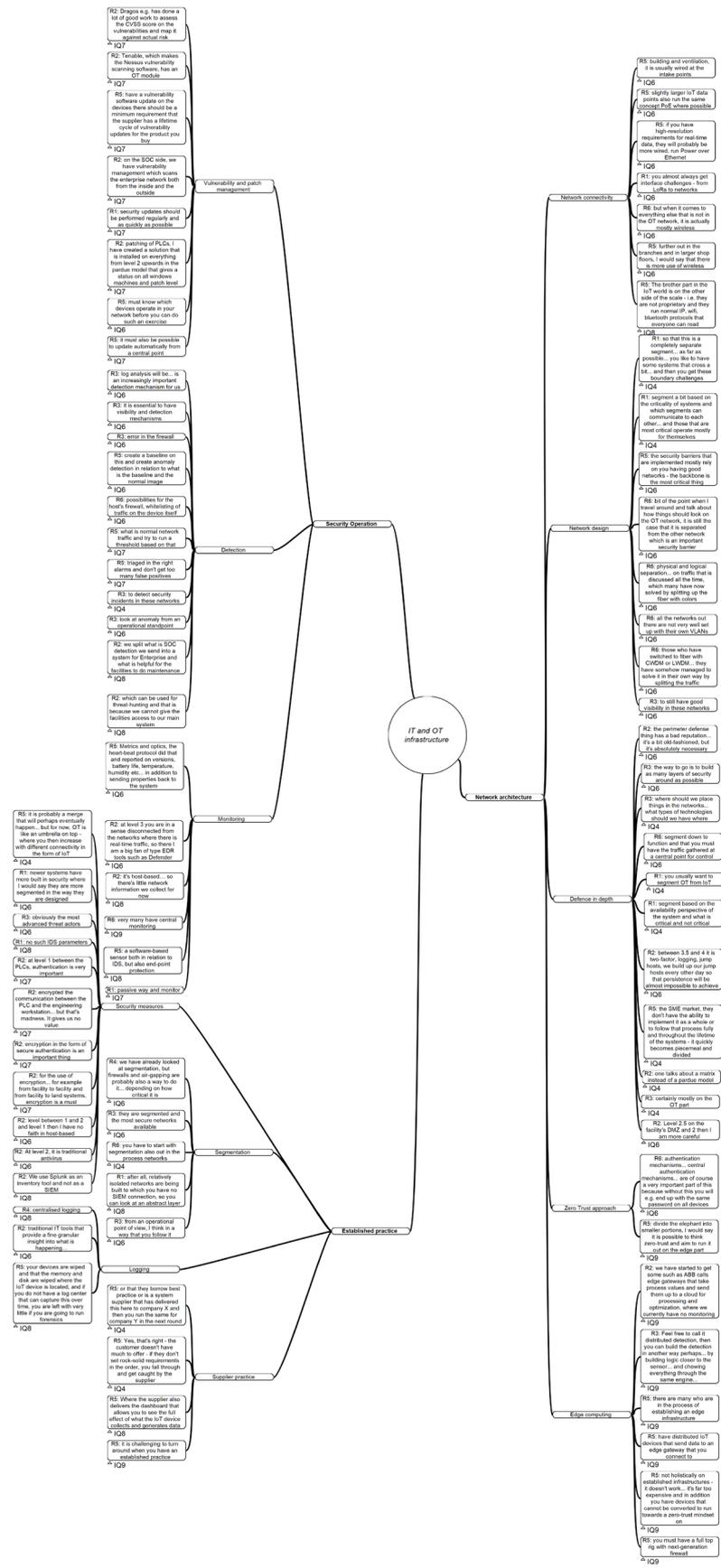


Figure E.2: The map of IT and OT infrastructure filtered for IQ4, IQ6, IQ7, IQ8 and IQ9

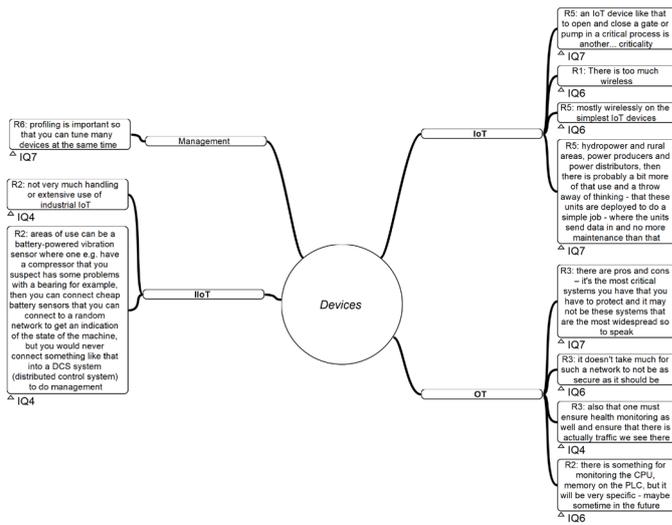


Figure E.3: The map of devices filtered for IQ4, IQ6, IQ7, IQ8 and IQ9

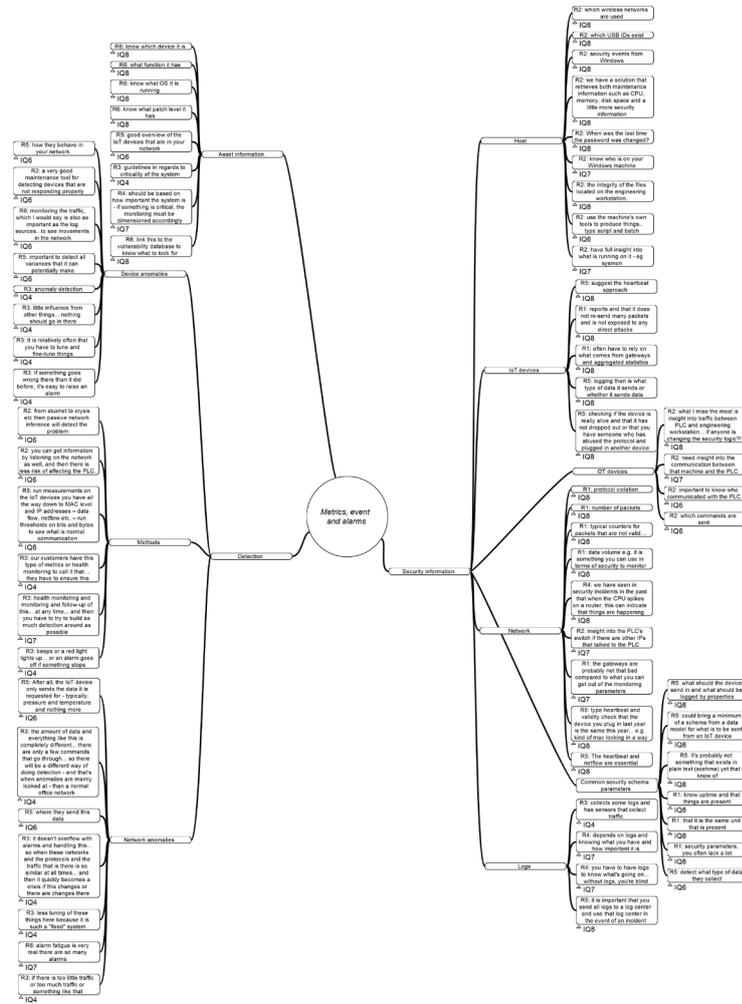


Figure E.4: The map of metrics, events and alarms filtered for IQ4, IQ6, IQ7, IQ8 and IQ9

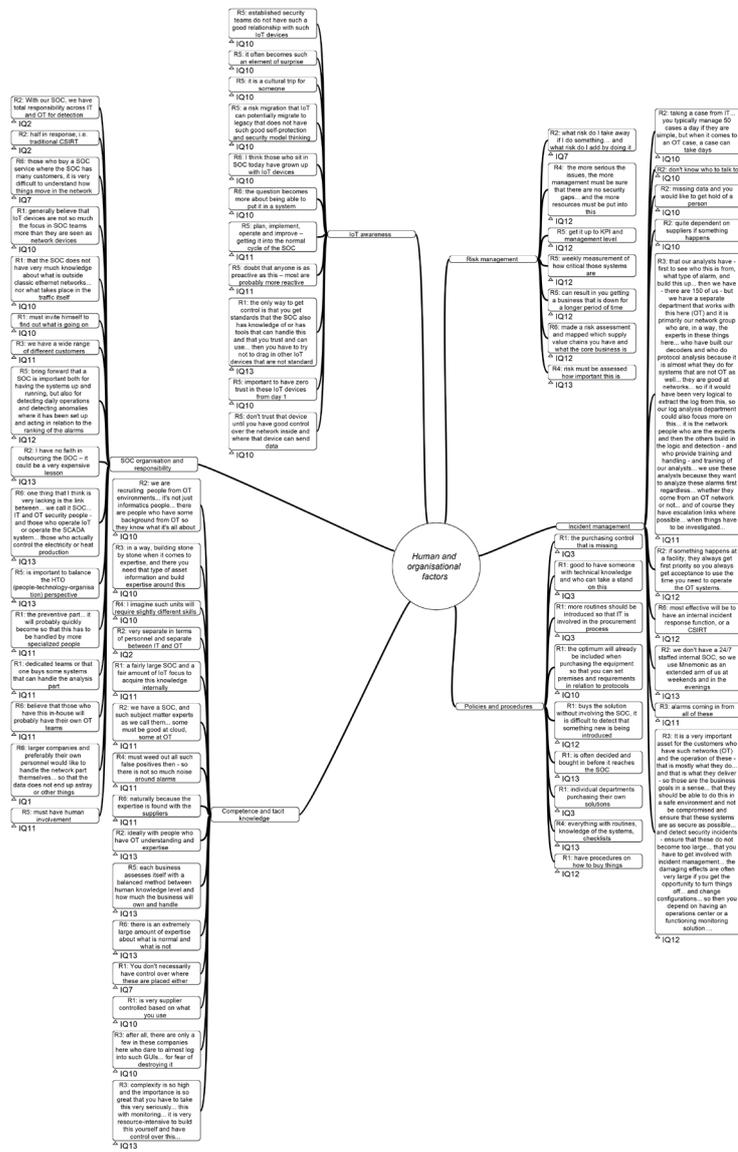


Figure E.5: The map of human and organisational factors filtered for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13

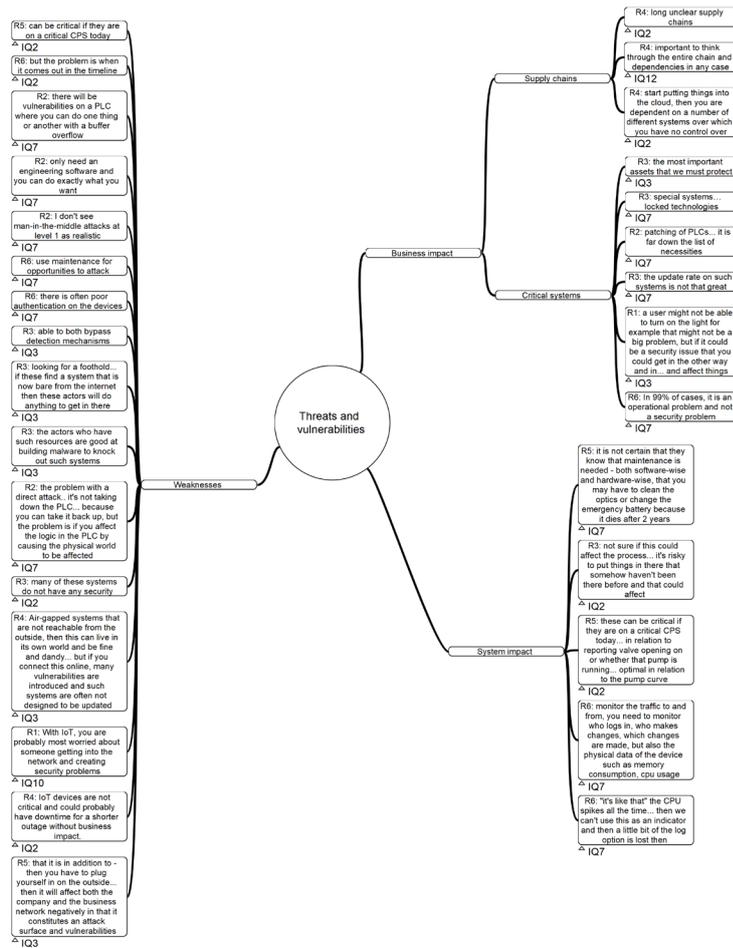


Figure E.6: The map of threats and vulnerabilities filtered for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13

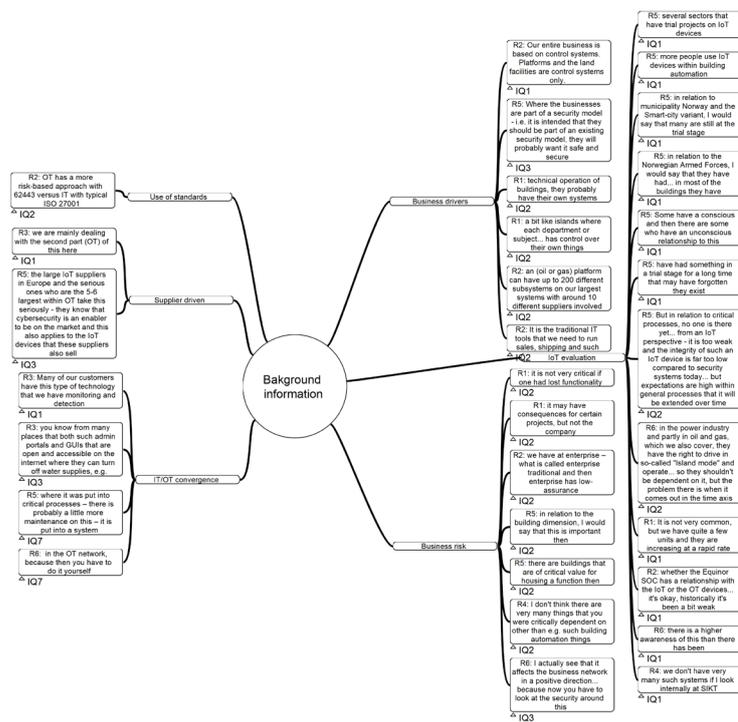


Figure E.7: The map of background information filtered for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13

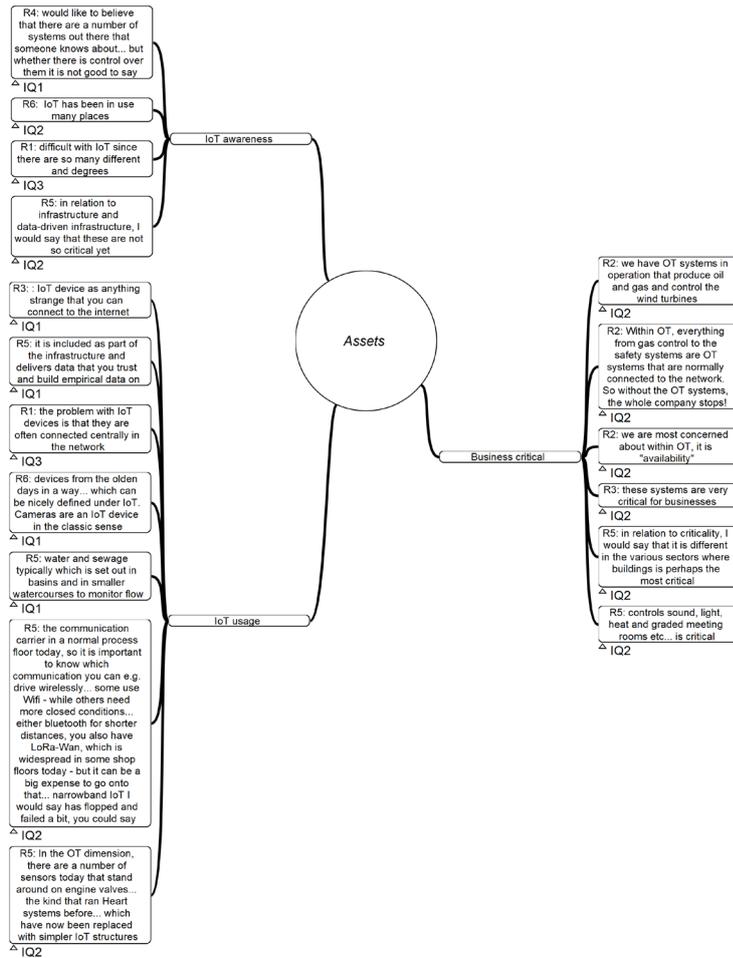


Figure E.8: The map of assets filtered for IQ1, IQ2, IQ3, IQ7, IQ10, IQ11, IQ12 and IQ13

Appendix F

A summary of state of the art aspects of SOC and IoT

Sorting			Aspects																																
			Monitoring		SOC Operating models		Software Architecture		Threats		Information aspect		Method		Device category (Sensor and Actuator)		Network		Communication		Protocols		Cyber Governance												
			SIEM Logging	SOAR	IDS	Monitoring	Internal SOC	Operational SOC	Microservice SOA	Industry 4.0	DDoSL	Malware	Physical attacks	Adversary Detection	Data (DA)	Attack detection	Assessment	Risk	Industry/IIoT	IoT	OT	Edge	5G	4G	MQAM	LoRa	Wi-Fi	MQTT	COAP	HTTP	ProSys	ProSys	Trust/ID/OW		
22	(Hadar & Hassanzadeh, 2019)	Big Data Analytics on Cyber Attack Graphs for Prioritizing Agile Security Requirements.	X																															X	
23	(Hassanzadeh & Burkett, 2018)	SAMIIT: Spiral Attack Model in IIoT Mapping Security Alerts to Attack Life Cycle Phases	X	X										X				X															X	X	
24	(Ferencz et al., 2021)	Review of Industry 4.0 Security Challenges	X	X	X					X	X	X						X															X	X	
25	(Hamad et al., 2020)	Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies									X	X	X		X			X		X														X	
26	(Tagarev & Sharkov, 2019)	Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems	X	X			X							X				X		X	X	X	X									X	X	X	
27	(Colelli et al., 2019)	Securing connection between IT and OT: The Fog Intrusion Detection System prospective	X			X								X	X			X		X	X					X	X								X
28	(Qiu et al., 2021)	Security Standards and Measures for Massive IoT in the 5G Era				X	X							X				X	X		X			X											X
29	(Bertino, 2019)	IIoT Security A Comprehensive Life Cycle Framework				X	X							X	X			X	X	X	X														X
30	(Yau Ti Duna, 2021)	Grasp on next generation security operation centre (NGSOC): Comparative study	X	X	X			X	X					X				X	X														X	X	X

Appendix G

Thematic Analysis

Year	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Number of projects	10	15	20	25	30	35	40	45	50	55	60	65	70	75
Number of projects completed	5	8	12	15	18	22	25	28	32	35	38	42	45	48
Number of projects in progress	5	7	8	10	12	13	15	17	18	20	22	23	25	27
Number of projects on hold	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Number of projects cancelled	0	0	0	0	0	0	0	0	0	0	0	0	0	0

