jamk

SOCs as Enablers for Continuous Threat Exposure Management

Risto Hookana

Master's thesis
March 2024
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Hookana, Risto

SOCs as enablers for Continuous Threat Exposure Management

Jyväskylä: Jamk University of Applied Sciences, April 2024, 92 pages.

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

Permission for open access publication: Yes

Language of publication: English

Abstract

Security Operations Centers or SOCs are in many organizations in a key role to protect against the cyber-attacks. SOCs need to be able to adapt and evolve to serve the business needs of the modern organizations, which digitalization can change in a fast pace.

Gartner, an IT research firm and a consultancy headquartered in United States of America, defines 'Continuous Threat Exposure Management' or CTEM as an "pragmatic and systemic approach to continuously adjust cyber-security optimization priorities" that utilizes technology, for example to align threat exposure assessments to business projects and threat vectors that are relevant to the organization.

The purpose of this research is to find what are the current capabilities that SOC possesses to support or enable a CTEM program in an organization. Other objectives are to recognize what capabilities CTEM is requiring in terms of People, Process and Technology Framework and what could be the potential gaps in SOCs capabilities to support CTEM. The research was carried out first by defining using literature what a SOC is and what it constitutes of and doing the same for CTEM. For CTEM, this work was done by using exclusively Gartner's subscribed client material. This was done with the consent and review of the chapters from Gartner. To recognize the capabilities that SOC possesses to enable or support a CTEM program, systematic literature review was used.

As a result of the research, two figures were created that answers all the three research questions that this thesis set out to answer. The thesis' results and thesis itself seem to be currently one of a kind in the world, as there were no observed academic publications mentioning CTEM during this thesis process.

Keywords/tags (subjects)

cyber security, cybersecurity, security operations center, SOC, security monitoring, detection, continuous threat exposure management, CTEM

jamk

Description

Hookana, Risto

SOCs as enablers for Continuous Threat Exposure Management

Jyväskylä: Jyväskylän ammattikorkeakoulu, huhtikuu 2024, 92 sivua.

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

Julkaisulupa avoimessa verkossa: kyllä

Julkaisun kieli: englanti

Tiivistelmä

Security Operations Center (SOC) tai turvallisuusvalvomot ovat monissa organisaatioissa avainasemassa kyberhyökkäyksiltä suojautumisessa. SOC:ien on kyettävä mukautumaan ja kehittymään palvellakseen modernien organisaatioiden liiketoiminnan tarpeita, jotka voivat muuttua nopeasti digitalisaation kehityksen takia.

Gartner, amerikkalainen IT-tutkimusyritys ja konsulttiyhtiö, määrittelee ’Continous Threat Exposure Managementin’ eli CTEM:n "pragmaattiseksi ja systemaattiseksi lähestymistavaksi jatkuvaan kyberturvallisuuden optimointiprioriteettien ohjaukseen" hyödyntäen teknologiaa, esimerkiksi sovittamalla uhka-altistumisen arvioinnit liiketoimintaprojekteihin ja uhkavektoreihin, jotka ovat relevantteja organisaatiolle.

Tämän tutkimuksen tarkoitus on selvittää, mitkä ovat SOC:in nykyiset kyvykkyydet tukea tai mahdollistaa CTEM-ohjelma organisaatiossa. Muita tavoitteita ovat tunnistaa, mitä kyvykkyyksiä CTEM vaatii People, Process, & Technology -viitekehyksen suhteen ja mitkä voisivat olla mahdolliset aukot SOC:ien kyvykkyyksissä tukea CTEM ohjelmaa. Tutkimus suoritettiin ensin määrittelemällä kirjallisuuden avulla, mikä SOC on ja mistä se koostuu, ja tekemällä sama CTEM:lle. CTEM:n osalta tämä tehtiin käyttämällä yksinomaan Gartnerin asiakkailleen tuottamaa materiaalia. Tämä tehtiin Gartnerin luvalla ja Gartner läpiluki myös kappaleet, joissa käytettiin heidän materiaaliaan. SOC:in nykyisten kyvykkyyksien tunnistamiseksi, joilla mahdollistetaan tai tuetaan CTEM-ohjelmaa, käytettiin systemaattista kirjallisuuskatsausta.

Tutkimuksen tuloksena luotiin kaksi kuvaa, jotka vastaavat kaikkiin kolmeen tutkimuskysymykseen, jotka tutkimus asetti. Tutkimuksen tulokset ja itse tutkimus vaikuttavat tällä hetkellä olevan ainutlaatuisia maailmassa, sillä CTEM:ää mainitsevia akateemisia julkaisuja ei havaittu tutkimusprosessin aikana.

Avainsanat (asiasanat)

kyberturvallisuus, security operations center, SOC, turvallisuusvalvonta, continuous threat exposure management, CTEM

Contents

List of abbreviations **4**
1 Introduction **5**
1.1 Background and motivation 5
1.2 Relevance of topic 6
1.3 Research questions 7
2 Research methodology **7**
2.1 Research method 8
2.2 Data collection 10
3 SOC definition and capabilities **12**
3.1 SOCs according to People, Process and Technology framework 15
3.2 People 16
3.3 Processes 20
3.3.1 Onboarding 22
3.3.2 Data collection 23
3.3.3 Detection and analysis 24
3.3.4 Incident management 25
3.3.5 Other processes 27
3.4 Technologies 31
3.4.1 Log collection 32
3.4.2 Security information and event management 34
3.4.3 Security orchestration, automation, and response 37
3.4.4 Endpoint detection and response 38
3.4.5 Other technologies 39
3.5 Summary of People, Processes and Technology for SOCs 41
4 Continous Threat Exposure Management by Gartner **42**
4.1 The five steps of CTEM cycle 46
4.1.1 Scoping 48
4.1.2 Discovery 50
4.1.3 Prioritization 53
4.1.4 Validation 55
4.1.5 Mobilization 57
4.2 Summary of the CTEM 59
5 Literature review of SOCs applicability to CTEM programs **61**
5.1 Data sources 61

5.2 Breakdown of CTEM PPT capabilities into search terms 62
5.3 Selection of publications 63
5.4 People applicability 67
5.5 Process applicability 68
5.6 Technology applicability 71
5.7 Summary of the literature review's results 73
6 Conclusion 73
6.1 Evaluation of reliability and ethicality of results 75
6.2 Suggestions for further research 76
References 77
Appendices 82
Appendix 1. Creation of search terms for literature review 82
Appendix 2. Selected publications and scoring 83
Appendix 3. Literature review results 85

Figures

Figure 1. Literature review process (adapted from Salminen 2023) 9
Figure 2. The PPT Framework (adapted from Prodan et al, 2015) 10
Figure 3. Integration between SOC and Client/Parent (adapted from Mutemwa et al. 2018) .. 15
Figure 4. Example of interactions of different roles within a SOC (adapted from Vielberth et al. 2020) 20
Figure 5. Threat intelligence process cycle (adapted from Bautista, 2018) 30
Figure 6. Typical SIEM components (adapted from Podzins and Romanovs, 2019) 36
Figure 7. EDR functionalities (adapted from Firstbrook et al., 2017) 39
Figure 8. Brief summary of PPT qualities of a SOC 42
Figure 9. Continous Threat Exposure Management by Gartner (2022a) 43
Figure 10. Do you have a CTEM Program? Gartner Peer Community Poll (2024a) 45
Figure 11. Continuous Threat Exposure Management by Gartner (2023b) 46
Figure 12. Example of Subscopes by Gartner (2023c) 49
Figure 13. Vulnerability Criticality by Asset Characteristic by Gartner (2023c) 51
Figure 14. Steps toward producing priortized and validated risk exposures by Gartner (2023c) 58
Figure 15. Recognized PPT capabilities of CTEM 60
Figure 16. Breakdown of CTEM PPT for literature review 62
Figure 17. PRISMA diagram for this thesis, adapted from Page et al. (2021) 66

Figure 18. Summary of literature reviews results....73

Tables

Table 1. Examples of possible SOC organizational models (adapted from Knerler et all., 2022)14
Table 2. SOC analyst responsibilities (adapted from Vielberth et al.2020)....17
Table 3. SOC role groups (adapted from Vielberth et al. 2020)....18
Table 4. Onboarding process (adapted from Onwubiko, 2021)....22
Table 5. Data collection process (adapted from Vielberth et al., 2020)....23
Table 6. Detection and analysis process phases (adapted from Vielberth et al. 2020)....25
Table 7. Incident management process (adapted from GovCERT.HK)....26
Table 8. High-level comparison of SIEM vs. log management system vs. data lake....33
Table 9. Scoping capabilities....50
Table 10. Discovery capabilities....52
Table 11. Prioritization capabilities....54
Table 12. Validation capabilities....56
Table 13. Mobilization capabilities....59
Table 14. Search terms used in Google Scholar during 9th and 10th of March 2024....63
Table 15. Questions presented to evaluate the quality of publications....65
Table 16. People applicability....67
Table 17. Process applicability....68
Table 18. Technology applicability....71

List of abbreviations

API	Application Programming Interface
BAS	Breach and Attack Simulation
CAB	Change Advisory Board
CISO	Chief Information Security Officer
CTEM	Continuous Threat Exposure Management
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
ECAB	Emergency Change Advisory Board
ECSF	European Cybersecurity Skills Framework
EDR	Endpoint Detection and Response
ETDR	Endpoint Threat Detection and Response
ENISA	European Union Agency for Cybersecurity
GRC	Governance, Risk and Compliance
I&O	Infrastructure & Operations
IoT	Internet of Things
IT	Information technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
PTaaS	Penetration Testing as a Service
PPT	People, Process and Technology
SaaS	Software-as-a-service
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
TDR	Threat Detection and Response
TI	Threat Intelligence
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures
WORM	Write-once, Read-many

1 Introduction

1.1 Background and motivation

In the rapidly evolving landscape of information technology and cybersecurity, the role of Security Operations Center, or SOC, is becoming increasingly critical. The capabilities of SOCs need to adapt and evolve as per the moving digital transformation, the new business opportunities, and the new ecosystems this transformation creates. Also, the continuously evolving cyber threats are seeking to utilize the weaknesses in these systems to gain monetary or intellectual benefits from them or to disrupt these systems. SOCs need to be able to adapt and evolve to serve the business needs of the modern organizations that are on the digital transformation journey.

SOCs often serve as the central hub in an organization's cybersecurity infrastructure, responsible for example monitoring, detecting, and responding to cybersecurity incidents. By and large, all medium and large organizations have some form of a SOC, and its significance is rising across various sectors, including business, government, and academia, as cyber operations become embedded to the daily operations of organizations. (Knerler et al., 2022)

Gartner (2023a) publication Top Strategic Technology Trends for 2024, presents a planning assumption that organizations that make their security investments based on the prioritizations made from their continuous threat exposure management (CTEM) program, will see a two-third decrease in cyber breaches affecting them by 2026. The publication defines CTEM as an *"pragmatic and systemic approach to continuously adjust cybersecurity optimization priorities"* that utilizes technology, for example to align threat exposure assessments to business projects and threat vectors that are relevant to the organization. The use of technology also includes the prioritization of organizations detected threat exposures utilizing the cyber attacker's point-of-view and validation of the planned security controls that address the exposure. The outcomes are used as evidence in the CTEM program to effectively engage several stakeholder teams to respond and optimize the organizations cybersecurity priorities. (Gartner, 2023a)

The main objective of the thesis is to understand if and how SOCs could enable the CTEM program or parts for it for an organization. This will involve defining and understanding what a SOC is and

what a CTEM is, understanding what these both consist of both and what could be the current possible gaps that SOCs could have to enable or support the organization's CTEM program.

The research carried out in this thesis can also provide insights to the process of conducting SOC tenders, with the aim of providing organizations both the information what they should consider their SOC provider offering and what SOC providers should think about offering to their clients. The results from this thesis can be utilized by both SOC service providers and organizations that are considering initiating a SOC tender, or organizations that are building or developing their own in-house SOC.

This research was conducted out of personal and professional interest of the author. The thesis will also leverage the author's practical experience in sales and service management of SOC services.

1.2 Relevance of topic

Researching the future requirements for SOCs is a topical research topic due to the increasing complexity and frequency of cyber threats, which drive the organizations to seek more advanced defense strategies. Moreover, SOCs role in addressing the global cybersecurity skills gap, helping or in some cases ensuring that organizations meet compliance and regulatory requirements, and SOCs reach around different sectors globally, emphasizes SOCs importance in not only addressing organization's cyber security concerns but also in strategically aligning with the future business objectives of organizations.

Therefore, the research related to SOCs by and large should consider not only how SOCs integrate new technologies like artificial intelligence and machine learning, but also how SOCs can better serve their end-clients by using the current technologies or what kinds of services SOC should offer to better support their clients in cybersecurity. This requires an understanding of the evolving business requirements of the organizations SOCs serve. Gartner forecasts that one of the developing business needs is the growing adoption of CTEM programs by organizations and thus it is the authors opinion that this deserves to be researched as one of the future possible development opportunities for a SOC.

SOC has been a highly featured subject in the academic literature, but during this thesis process academic literature of how SOC and CTEM interconnect was not found. Also, not a single academic publication featuring or mentioning CTEM was found. This leads to the conclusion that the research set out for this thesis has also the possibility for producing unique academic knowledge.

1.3 Research questions

The research questions for this thesis are:

- **RQ1:** What are the current capabilities that Security Operations Centers (SOCs) possess to effectively support Continuous Threat Exposure Management (CTEM) programs?
- **RQ2:** What CTEM requires in the people, process, and technology point-of-view?
- **RQ3:** What can be the gaps in SOC capabilities for participation to CTEM?

The research questions are guiding the thesis work. They are also separate tasks which the author seeks to find the answers during the thesis research.

2 Research methodology

The selected research method for this thesis is qualitative research and the research will employ a literature review and the usage of the People, Process and Technology Framework. The literature review will involve the examination of academic and industry publications, and whitepapers. The purpose of the literature review is to see if the recognized capabilities for an CTEM program are existing also in the literature for SOCs.

Hirsjärvi et al., outline three traditional research approaches: experimental, quantitative, and qualitative. Experimental research involves measuring how variables interact under various conditions, often testing specific hypotheses. Quantitative research typically uses surveys or structured interviews to collect standardized information from a population, aiming to describe or elucidate phenomena. Qualitative research focuses on obtaining detailed data from individual cases or groups, primarily to describe a particular phenomenon. Hirsjärvi et al., state that researchers need to align their choice of research strategy and methods with their research questions. (Hirsjärvi et al., 2010)

According to Hirsjärvi et al., the aim of qualitative research is to accurately depict reality and comprehensively explore the topic of study. In qualitative research, there is a connection between the researcher and the subject's known aspects, making it unfeasible to achieve an objective viewpoint. Because of this, the findings of the qualitative research are limited to a specific time and a location. Also, rather than confirming pre-existing hypotheses, the goal in qualitative research primarily focuses on uncovering or discovering new facts regarding the researched subject. (Hirsjärvi et al., 2010)

2.1 Research method

The semi-systematic review was selected as the literature review method due to its balance between systematic structure and flexibility. According to Snyder, semi-systematic review approach is particularly suitable for exploring broad topics that have been conceptualized differently across various disciplines, allowing for a comprehensive overview and identification of themes, theoretical approaches, and knowledge gaps. Unlike systematic reviews, which require strict adherence to predetermined protocols, the semi-systematic review offers flexibility to adapt to the interdisciplinary nature of the research area, making it an effective strategy for mapping out the field and synthesizing diverse perspectives. (Snyder, 2019)

Salminen states that the benefits of literature review are that it offers an opportunity to process and summarize extensive materials, generating new knowledge that contributes to the understanding of a scientific field. According to Salminen, literature review compels the researcher to engage with the discourse in their field over an extended period, and to find content that is justifiable for their own discipline. (Salminen, 2023)

According to Snyder, a variety of guidelines exist for conducting literature reviews. The used methodology should be selected as per the objective of the literature review. These methodologies may adopt a qualitative, quantitative, or mixed-methods approach, varying with the review's stage. Three widely recognized methods are systematic reviews, semi-systematic reviews, and integrative reviews. In appropriate contexts, each of these strategies can provide substantial assistance in addressing a particular research question. (Snyder, 2019)

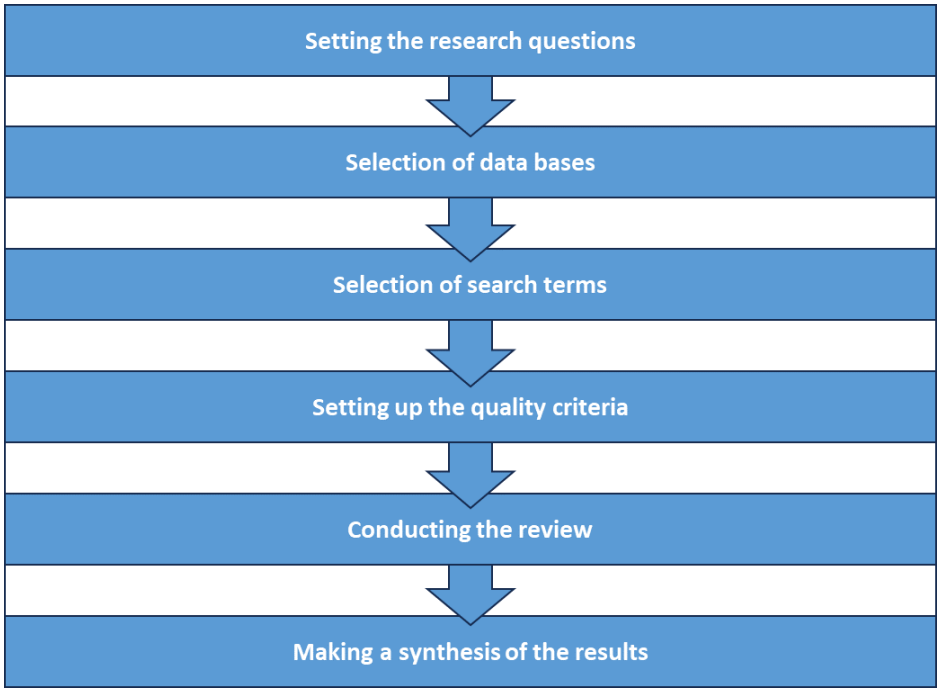

Figure 1. Literature review process (adapted from Salminen 2023)

As stated in the introduction, the objective of the research is to understand what capabilities SOC should have at their disposal to support CTEM programs. To achieve this, it will be paramount to research and understand what both SOC and CTEM are and what are the 'factors of production' that both require. As SOCs are organizations themselves, they have a multitude of capabilities and characteristics which all effect to what kind of services and in what capacity the SOC organization can provide its end-clients. When assessing the capabilities of an organization, a commonly used framework is the People, Process, Technology framework.

The People, Process, Technology (PPT) framework is a holistic organizational model emphasizing the interconnection of people, processes, and technology for optimal performance and problem-solving. The emphasis is that for an organization to thrive, equal attention must be given to the human element (People), the methods and practices employed (Process), and the tools and infrastructure used (Technology). People are central, focusing on skills, training, and culture to effectively utilize technology and execute processes. Processes are the structured approaches and policies that guide and optimize the interaction between people and technology. Technology refers to the tools and systems that support and enhance the capabilities of the people and the effectiveness of the processes. (Prodan et al., 2015)

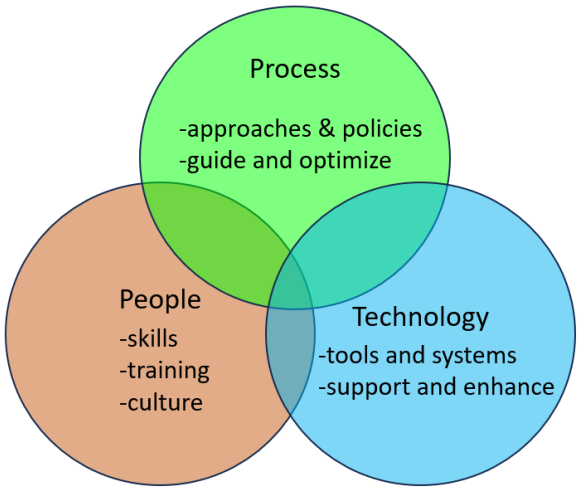

Figure 2. The PPT Framework (adapted from Prodan et al, 2015)

2.2 Data collection

Regarding the data collection methods, Hirsjärvi et al. state that qualitative research involves extensive data collection that is done in natural settings, prioritizing people as the primary information source. In qualitative research, researchers rely more on direct observations and conversations with subjects than on data obtained from tests or surveys. That is why qualitative research emphasizes methods that highlight the subjects' personal perspectives and beliefs. This aligns with the careful selection of specific target groups for data gathering in qualitative research. (Hirsjärvi et al., 2010)

Regarding the study of the definition and capabilities of a continuous threat exposure management or CTEM, this thesis will use Gartner's publications for their subscribed users regarding the CTEM program. Gartner is an IT research firm and a consultancy headquartered in United States of America. Gartner operates worldwide and it listed in the New York Stock Exchange. The company operates globally, offering data visualization, analysis tools, and consulting on strategy development, technology selection, and implementation. One of the most known tools Gartner offers is the Gartner Magic Quadrant, which tracks and analyzes companies in a specific technology market. (*What Is Gartner?*, n.d.)

While Gartner's reports and analyses might not follow the traditional scientific methodology characteristic of academic publications, they offer a pragmatic perspective that is meant to address the

operational realities and strategic considerations of organizations. Expert organizations can have significant influence in the IT and cybersecurity sectors, with its findings often serving as benchmarks for industry standards and best practices. These expert organizations can affect the strategies, challenges, and technological advancements that organizations worldwide follow and implement.

Gartner's consent to use their subscribed material for this thesis was requested and consent was obtained. The chapters where Gartner material was utilized were reviewed and approved by Gartner in March 2024.

The data collection method for the research regarding SOCs capabilities to support organizations CTEM program is literature review. According to Salminen, the fundamental concept of a literature review is to conduct 'research on research'. When research information is compiled and processed, these actions lay the groundwork for new research findings. A literature review falls into the category of combining qualitative and quantitative methods (i.e., a mixed method approach). (Salminen, 2023)

Salminen lists five goals of literature review, which according to Salminen are firstly, to develop existing theory and to also construct new theory. Secondly, the review enables the evaluation of theory. Thirdly, a literature review creates a comprehensive picture of a certain subject matter. Fourthly, the review aims to identify problems. Fifthly, a literature review offers the opportunity to historically describe the development of a specific theory. (Salminen, 2023)

Hirsjärvi et al. state, that the information collected is treated as unique, and its analysis is tailored accordingly. At this stage, inductive analysis is applied to the data, leading to generalizations and conclusions aimed at uncovering surprising findings. The focus in qualitative research is on a comprehensive and multi-leveled examination of the collected data, rather than on verifying any pre-established theories or hypotheses. Additionally, in qualitative research, the research plan is dynamic, evolving and morphs itself into its ultimate form as the research progresses. (Hirsjärvi et al., 2010)

3 SOC definition and capabilities

The first-generation of SOCs emerged with the birth of the Internet during 1970s. This was also a time when most organizations lacked network defense measures. As Internet adoption grew, so did the exploitation and abuse of online resources. Early detection efforts of cyber threats and attacks relied on creative thinking of the cyber defense personnel but lacked organization and the detection methods and tactics were often not repeatable. By the mid-1980s, cyber threats gained public attention through media and government channels. Initial security tools like antivirus, firewalls, proxies, and intrusion detection systems appeared. The first 'security operations' took shape to oversee these tools and respond to threats. Typically led by a single individual with a networking background, these early security operations paved the way for the emergence of formal SOCs, primarily in government and military sectors. Analysis of incidents in these SOCs was often unstructured and bandwidth to deal with different incidents was limited. (*5G/SOC: SOC Generations*, 2013)

Knerler et all. (2022) state that the cybersecurity operations have evolved significantly since the early days. Over time, the cybersecurity community has enhanced its understanding of cyber adversaries. Initially, SOCs primarily focused on detecting cyber incidents and adversaries during active reconnaissance or active attacks. However, today's SOCs must broaden their situational awareness. In an ideal scenario, SOC should be integrated into a larger cybersecurity initiative in the organization, that comprehends cyber adversaries well enough to prevent or mitigate attacks before they happen or detect incidents before substantial damage takes place. (Knerler et al., 2022)

In terms of what constitutes as a SOC, Knerler et all. (2022) state that *"SOC is defined primarily by what it does: cyber defence"* and they continue to define SOC as follows: *"A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents*". There are also a varied range of services and support roles a SOC may undertake, including developing its own tools or gathering cyber threat intelligence, although not every SOC may offer all these services. (Knerler et al., 2022)

Kokulu et all. (2019) define SOC as a unit dedicated to defending an organization's computing environment. This defense is achieved using various tools, technologies, and processes. SOCs can be

internal SOCs, which are operated and managed within the organization they defend, and out-sourced SOCs, which are independent entities paid for SOC services by the organization. A SOC may be known by different names, such as Cyber Security Operations Center (CSOC), Computer Security Incident Response Team (CSIRT), or Information Security Operations Center (ISOC). (Kokulu et al., 2019)

According to Vielberth et all. (2020) SOC can also be defined as an organizational unit operating at the core of all security operations. It is not typically viewed as a single entity or system, but rather as a complex structure designed to manage and enhance an organization's overall security posture. The primary functions of a SOC are to detect, analyze, and respond to cybersecurity threats and incidents, utilizing a combination of people, processes, and technology. (Vielberth et al., 2020)

Knerler et al., 2022, conclude that there is no single universally accepted term for SOC and its composition and the preferences for different terms can vary over time, by country, and according to the SOC team's specific mission. Fundamentally, the essential functions of a SOC revolve around detecting, analyzing, and addressing security breaches, which are central to the SOC's primary mission. Regarding the organizational model of a SOC, there is no single standardized organizational structure for a SOC that would serve all the different needs of different organizations. (Knerler et al., 2022)

Table 1. Examples of possible SOC organizational models (adapted from Knerler et all., 2022)

Organizational model	Typical organizations utilizing the SOC model	Considerations
Ad Hoc Security Response	Small organizations	No proactive incident detection or response; resources are gathered as needed for incident resolution, leading to varied outcomes due to a lack of centralized expertise and defined processes.
Security as Additional Duty	Small businesses and small organizations e.g. local governments	Security responsibilities are integrated into other roles, like system administration, without a formal SOC structure; limited incident response procedures may exist.
Distributed SOC	Small to medium-sized organizations	Formal SOC authorities with resources dispersed across the organization; staff may have additional duties.
Centralized SOC	Wide range of organizations including medium to large-sized businesses, educational institutions (such as a university), or government agencies	Security operations are consolidated under one authority and organization with dedicated SOC roles; the most common and straightforward SOC model.
Federated SOC	Organizations with distinct operating units that function independently of one another such as businesses that have acquired other businesses but have not integrated them together	Multiple independent operating units share a SOC structure, potentially centralized or hierarchical, with some shared policies and authorities.
Coordinating SOC	Large organizations or government institutions	Large organizations have a coordinating SOC that manages overall incident management and coordinates other SOCs, without direct day-to-day oversight.
Hierarchical SOC	Large organizations or government institutions	Similar to Coordinating SOC, but the parent organization plays a more active role, offering SOC services and coordinating a broader range of SOC functions.
National SOC	Country level governments	Country-level government entity responsible for enhancing national cybersecurity by facilitating information sharing and coordinating responses to significant cyber incidents.
Managed Security/ SOC Service Provider	Organizations of all sizes	Delivers security services to external entities through a business arrangement based on fees or charges.

Knerler et al. state that the acronym "SOC" was decided to be used in their publication to describe these cybersecurity teams, regardless of their various forms and sizes. Also, for the purposes of

this thesis, the only used name of the abovementioned groups or organizations consisting of cybersecurity experts that are focused on detecting, analyzing, and responding to cyber incidents shall be SOC.

3.1 SOCs according to People, Process and Technology framework

Studies frequently outline the functioning of a SOC by using the People, Processes, and Technologies (PPT) framework. This framework is also applied to a range of information technology subjects, including knowledge management and customer relationship management. Additionally, it is a common approach among SOC vendors to organize and describe their products using this framework. (Vielberth et al., 2020)

SOCs themselves have people, processes, and technologies, which need to be aligned with the counterparts of their clients or parent organizations. The primary challenge arises when an organization introduces cybersecurity, and key stakeholders responsible for system technologies and processes may not fully comprehend their roles in cybersecurity. SOC's integration into the organization may initially be perceived as close job monitoring by these stakeholders. To address these concerns, it is essential to conduct kickoff meetings with all relevant system technology and process stakeholders to clarify that SOC personnel are there to enhance security. (Mutemwa et al., 2018)

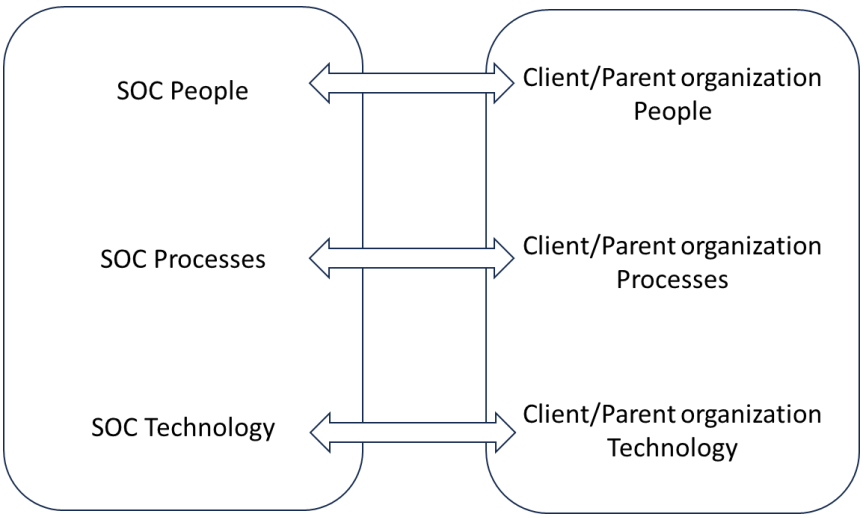

Figure 3. Integration between SOC and Client/Parent (adapted from Mutemwa et al. 2018)

As mentioned in chapter 2, Research Methodology, the following sub-chapters will define the typical composition and the capabilities of SOC by using the PPT framework. The idea is not exhaustively present all the possible characteristics a SOC may have in all the three domains of PPT framework. The idea is to rather highlight what prevalent characteristics there is mentioned in academic literature that would be most likely present in the different modern SOCs outlined in the Table 1. Examples of possible SOC organizational models.

3.2 People

Related to the multitude of different services and thus people a SOC may or may not have, Knerler at al. point out that different organizations may perform a variety of functions or services within a SOC, but not all organizations will necessarily conduct all those functions utilizing SOC. If a SOC focuses primarily on core activities like real-time alert monitoring and incident triage, it is likely to have a simpler organizational structure with fewer teams compared to a SOC that also offers services such as vulnerability scanning, penetration testing or threat hunting. It is paramount to understand and distinguish between the services that the SOC provides and the security services that other parts of the organization or external entities offer. The defense of the organization is a collective responsibility that involves multiple stakeholders. (Knerler et al., 2022)

The career progression and job roles within a SOC depends on how the organization assigns responsibilities to the job roles. Entry-level positions in networking, software development, system engineering, and security intelligence can transition into roles like junior analyst, consultant, or tester within the SOC. As experience and compensation grow, individuals can advance to positions such as senior architect or security administrator. It's important to note that there is no standardized career path or uniform requirements across organizations. Job titles and qualifications can vary widely from one organization to another, even for similar roles. Different organizations may have specific certification, degree, or experience requirements for the same job title. (Muniz, 2021)

A primary function of a SOC is to consume and analyze data relevant to cyber incidents. These incidents, observed on the company's network and endpoints, often necessitate additional action. A dedicated team within the SOC, known as SOC analysts, is responsible for the real-time assessment of these alerts, logs, and events. Usually, SOCs have three or more teams of analysts that are

divided into what is called tiers. Generally, the higher the tier level, the more specialized the analysts' responsibilities become. Additionally, there is a variance in the expected resolution time for incidents at each tier. Analysts at lower tiers are anticipated to resolve incidents more quickly compared to those at higher tiers, as escalated incidents are typically more complex. (Kokulu et al., 2019)

Vielberth et al. have produced the following list of the tasks and responsibilities of three tiers of SOC analysts:

Table 2. SOC analyst responsibilities (adapted from Vielberth et al.2020)

Tier	Role	Responsibilities
Tier 1	Triage Specialist	• Analyze incoming alerts. • Assess and adjust alert importance, adding relevant data to them. • Determine alert legitimacy and identify high-risk events or potential incidents, prioritizing them. • Escalate unresolved alerts to tier 2 analysts.
Tier 2	Incident Responder	• Assess more serious security incidents forwarded by tier 1. • Utilize threat intelligence tools. • Investigate the scope of an attack and affected systems. • Translate basic attack data into actionable intelligence. • Develop and apply incident management and recovery strategies. • Escalate complex issues as needed.
Tier 3	Threat Hunter	• Handle significant alerts escalated from tier 2. • Conduct or oversee vulnerability assessments and penetration tests to uncover potential attack methods. • Proactively identify unknown threats, security weaknesses, and vulnerabilities. • Recommend enhancements for security monitoring tools. • Review critical security alerts, threat intelligence, and security data from tiers 1 and 2.

However, Knerler at al. state that the tiered structure is not universal across all SOCs. Each SOC is unique, leading to differing opinions among professionals about the most effective operational structure. While SOCs without a tiered system might adopt a function-based organizational structure, those with a larger team of analysts often find tiering necessary and beneficial for meeting

their goals and operational needs. Success is possible with either approach, provided distinct recruiting and staff development strategies are followed. (Knerler et al., 2022)

Vielberth et al. have identified four other additional role groups and different job titles within those role groups in addition to the SOC analyst roles. All these roles and titles can be at some extent be involved in the daily operations of a SOC. These additional roles need to lead, work together, or cooperate with the previously described core SOC analyst roles for successful SOC operations. (Vielberth et al., 2020)

Table 3. SOC role groups (adapted from Vielberth et al. 2020)

Management Roles:	
SOC Manager	A person that takes charge of overseeing the SOC's operations and managing the security operations team. Tasks include e.g. hiring, training, evaluating team members, creating processes, and assessing incident reports. Managers oversee financial matters, provide support to security audits and report to the Chief Information Security Officer.
Chief Information Security Officer (CISO)	Responsible for formulating an organization's security strategies, goals, and overall security operation objectives. Note that the CISO can also be a Client representative to the SOC, if the SOC is a managed security services provider that offers SOC services to clients in exchange for monetary compensation.
Incident Response Coordinator	Whose primary responsibility is to coordinate all activities related to incident response in a high-level management capacity.
Technical Roles:	
Malware Analysts	Responding to sophisticated cyber threats by engaging in malware reverse engineering and generating essential insights and threat intelligence to be used in incident response efforts.
Threat Hunters	Proactively seek out cyber threats within the organizations, such as by reviewing logs, or externally by analyzing available threat intelligence data.

Threat Intelligence Analysts	Analyze the threat intelligence data and provide valuable input by e.g. creating and sharing indicators-of-compromise to the SOC team.
Forensic Specialists	Conduct forensic investigations to successful cyber-attacks by collecting and analyzing forensic evidence in a manner that follows legal standards for forensic evidence handling.
Red/Blue Teams	Attempting to attack and defend the organization's systems, with the goal of identifying vulnerabilities and enhancing the effectiveness and resilience of security mechanisms.
Vulnerability Assessment Experts	Do research to identify new, previously undiscovered vulnerabilities, as well as manage known vulnerabilities while considering their impact on business risk. These experts produce detailed technical reports based on their findings and offer support to SOC analysts or incident response teams in addressing identified vulnerabilities.
Security Engineers	Responsible for developing, integrating, and maintaining SOC tools, as well as defining requirements for new tools. They ensure appropriate access to tools and systems and handle tasks such as configuring and installing firewalls and intrusion detection/prevention systems. Furthermore, they assist in creating and updating detection rules for Security Information and Event Management (SIEM) systems.
Consulting Roles:	
Security Architect	Responsible for strategizing, researching, and crafting a resilient security infrastructure within the company. Security architects routinely conduct system assessments and vulnerability tests, and they either implement improvements themselves or oversee their implementation. Additionally, they are tasked with establishing recovery procedures.
Security Consultants	Engaged in researching security standards, best practices, and security systems. They can provide organizations with an industry-wide perspective and can compare the current capabilities of the SOC with those of competitors. Furthermore, they can assist the security architect in their work.
External Roles: **Personnel from outside the SOC organization can be integrated into various aspects of SOC operations.**	

As it was mentioned by Vielberth et al., below is an example figure that illustrates the different possible interactions these different SOC role groups would have in a day-to-day SOC operations context. As it was also mentioned earlier in the chapter, some of the roles may not exist in some SOCs or some additional roles may exist on top of these in another SOC. It eventually comes down to the objective of the SOC and what type of service its stakeholders and clients are expecting the SOC to be able to provide.

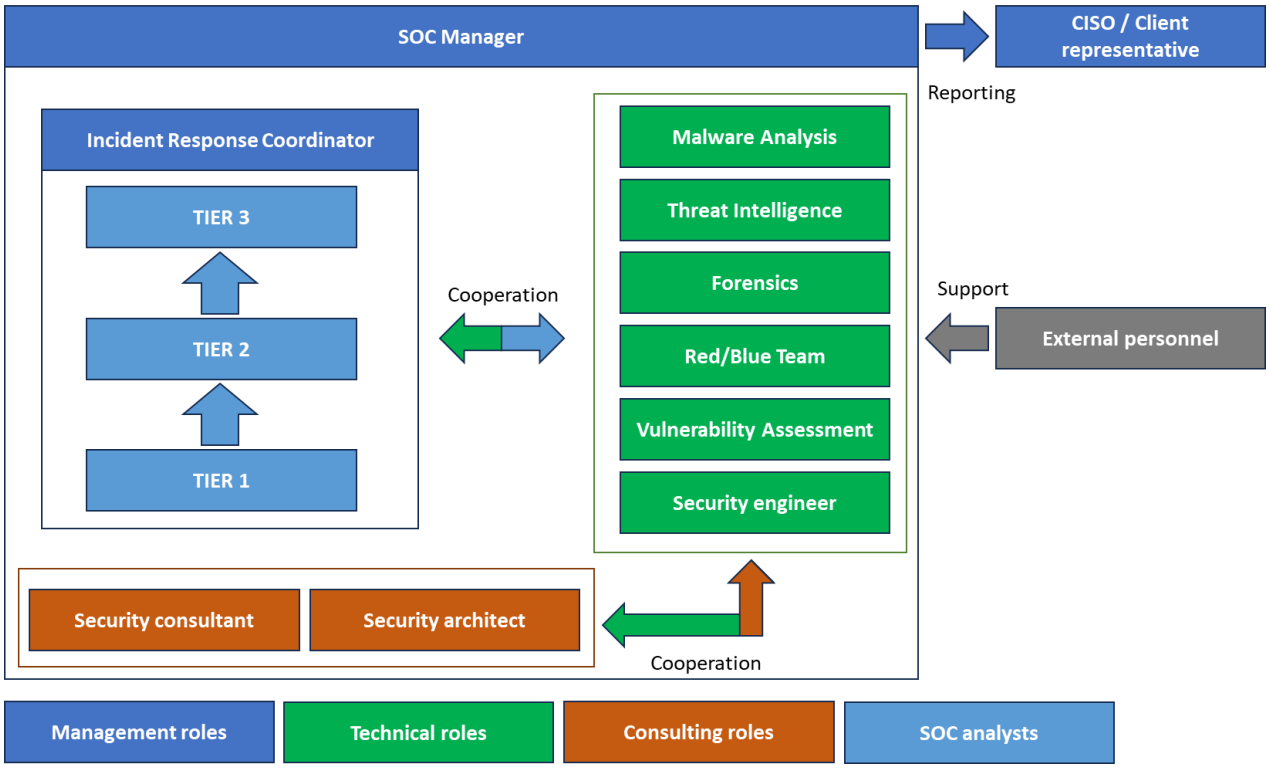

Figure 4. Example of interactions of different roles within a SOC (adapted from Vielberth et al. 2020)

3.3 Processes

According to Mutemwa et al. (2018), in a SOC, a process refers to the series of actions taken to resolve a security incident. On the other hand, within an organization, a process pertains to the steps followed to address e.g. help desk calls, considering the calls' priorities. To assess the SOC's Return on Investment and generate reports effectively, it is crucial to integrate SOC processes with those of the client or parent organization. This integration includes aligning SOC processes as

closely as possible with the organization's procedures and utilizing shared systems whenever feasible. (Mutemwa et al., 2018)

The definition of Mutemwa et al., that processes in SOC are related to resolving security incidents is probably the most common. However, Vielberth et al., state that review has revealed a significant gap in the literature concerning SOC processes. Given that these processes are fundamental to understanding SOCs and effectively implementing them, the absence of well-defined processes hinders academia from gaining a complete understanding of what organizations do within a SOC. On the other hand, it becomes challenging to identify areas for even minor enhancements, let alone innovations, at a conceptual level. This lack of abstract, high-level insight into SOC processes often leads many researchers to concentrate on enhancing technologies without a clear comprehension of which specific process or task within a SOC requires improvement. (Vielberth et al., 2020)

This is also the conclusion Villalon-Huerta et al., arrived to. Villalon-Huerta et al., argue that in the People, Processes and Technologies model, the processes are not standardized in the literature and do not reflect what actions SOCs perform to conduct their daily operations. According to Villalon-Huerta et al., regarding the definition of processes in a SOC, many approaches prioritize incident handling processes, often neglecting critical aspects such as data acquisition and data processing, which are treated as secondary. This focus results in well-established models for incident response once an incident is detected, but it lacks a unified approach to the essential preceding tasks. Additionally, approaches centered on incident response overlook a crucial concept: not all response activities in a SOC are tied to this process. Response actions can vary based on numerous factors, both technical (e.g., incident priority or potential impact) and non-technical (e.g., contractual obligations with specific customers). (Villalon-Huerta et al., 2022)

Vielberth etl al, continue that gaining a clear comprehension of SOC processes, tasks, and interactions necessitates their integration with other organizational processes. This gap needs to be addressed by academia to achieve a comprehensive understanding of SOC operations. Only then can the ongoing growth of SOCs be sustained effectively. Vielberth etl al, note that "post-incident activity" remains underexplored in SOC literature, despite its significant role in learning and continuous improvement. (Vielberth et al., 2020)

What could be argued to be among the initial processes in the client or parent organization point-of-view in regards with a SOC would be the onboarding process.

3.3.1 Onboarding

SOCs must onboard the client or parent organization business services to their monitoring to provide them with cyber defense services. Onboarding is a technical process of configuring the systems to generate appropriate outputs for the security monitoring technologies utilized by SOCs. This can include e.g. events, logs, messages, metrics, and other observables. Correlation and analysis are then used to these outputs to determine whether a cyber incident or attack is taking place. (Onwubiko, 2021)

Onwubiko continues that the common procedure for a SOC onboarding an organization into continuous security monitoring has four phases which are *discovery, solutions design, implementation,* and *risk assurance*.

Table 4. Onboarding process (adapted from Onwubiko, 2021)

Onboarding process phase	Description of activities in the phase
Discovery	During this phase, the SOC collaborates with business stakeholders and asset owners to gain insights into their specific business requirements. During this phase it is important to recognize that these business requirements can vary significantly among different types and sizes of organizations.
Solutions design	Designing how and to which security monitoring systems the SOC will ingest the outputs from the source systems and business services.
Implementation	The solutions design is implemented, and testing is conducted, including integration testing, business unit testing, end-to-end testing, and service acceptance testing.
Risk assurance	Measures such as penetration testing can be also carried out, and documentation is prepared for accreditation, certification, or attestation protocols to ensure that any possible errors or misconfigurations done during the onboarding are recognized and handled.

The SOC onboarding is a crucial initial step in the point of view of the client or the parent organization. Understanding the business drivers and requirements and the security monitoring needs that are created by them is paramount to be able to create a successful SOC service. For instance, one organization may have a business imperative to ensure the security monitoring of their digital and online payment transactions. On the other hand, a financial institution, such as a bank, might prioritize monitoring its internet banking services, while a government department could be mandated to safeguard citizens and national critical infrastructure. (Onwubiko, 2021)

3.3.2 Data collection

The sequence of the data collection process steps is not standardized across the literature. This can be explained by the fact that the process will change according to the application where the data shall be collected. The data collection phases are however usually presented in the sequence that is showcased in the table below. (Vielberth et al., 2020)

Table 5. Data collection process (adapted from Vielberth et al., 2020)

Data collection process phase	Description of activities in the phase
Data ingest to SOC	The selected system output data is collected via technological means to be consumed in the security monitoring provided by the SOC. The data collection methods are planned and implemented in the onboarding phase.
Normalization	The phase involves transforming diverse data formats into a uniform representation, including synchronizing time data to one time zone and format to prevent timeline confusion in security monitoring analysis. This process can be referred also as log parsing or pre-processing.
Filtering	Selecting the data elements with significant security relevance to be consumed into the SOC security monitoring. This is paramount as the systems can generate vast volumes of data.
Reduction	Incoming output data from systems is further reduced so that only important data fields from the output are collected.
Aggregation	Combining similar output events into a single data element; for instance, multiple log entries about a login attempt can be merged into one, indicating the type and count of login attempts.

Prioritization	Classifying the output data from systems based on the system and/or event priority to help prioritize further analysis and decision-making, such as event response or data retention duration.

Regarding data collection, while informal agreements with system owners and sysadmins may have fast and effective results, the long-term data collection can be compromised by potential personnel changes. For medium to large organizations, formalizing arrangements through a Memorandum of Agreement (MOA) or Understanding (MOU) is beneficial for establishing significant data feeds or specific monitoring initiatives. Formal documentation of monitoring requirements often leads to improved satisfaction by setting clear service expectations. A data collection memorandum typically outlines technical and management contacts, data collection and usage specifics, audit and retention responsibilities, security measures, collection tools, and additional SOC and system owner expectations. (Knerler et al., 2022)

3.3.3 Detection and analysis

The data collected in the previous processes needs to be further processed to provide value as means to conduct cyber defense to an organization. Transforming this data into valuable insights is achieved through data analysis. Vielberth et al. state that in the context of automatic analysis and detection, the existing literature mainly concentrates on specific methods and technologies for analysis and detection. Based on the literature the phases for detection and analysis process are *detection, analysis,* and *alert prioritization/triage*. (Vielberth et al., 2020)

SOCs can receive initial incident reports through various channels, including email, phone, IT service desk tickets, partner organizations, and their own monitoring tools. Analyst teams then assess these reports to determine the appropriate next steps. Often, what is initially reported as anomalous or unexplained activity may not immediately be recognized as an incident, creating a challenge for accurate categorization. A mutual arrangement between the IT help desk and SOC might mandate that all security-related concerns handled by the help desk, such as phone calls and tickets, are immediately redirected to the SOC for escalation and further action. (Knerler et al., 2022)

Table 6. Detection and analysis process phases (adapted from Vielberth et al. 2020)

Detection and analysis process phases	Description of activities in the phase
Detection	Incidents are identified either through human intervention or automatic procedures, and a determination is made as to whether the collected data signals about a security incident.
Analysis	Analytical techniques can be categorized into source and target correlation, structural analysis, functional analysis, and behavior analysis. The purpose of correlation is enabling the analysis of complex chain of events by generating simplified and accurate incidents.
Alert prioritization / Triage	Serves as the prior phase before the containment, eradication, and recovery from the incident. This phase serves two primary objectives: prioritizing the handling of the most severe incidents and ensuring that incidents are distributed for further processing.

3.3.4 Incident management

This process aims to differentiate between non-harmful events (e.g., during penetration testing) and cyber incidents. If a cyber incident is identified, it is escalated to the relevant parties for further action. The typical phases in incident management process are containment, eradication, and recovery. (Vielberth et al., 2020)

According to the Government Computer Emergency Response Team of Hong Kong (GovCERT-HK, 2023), the containment, eradication, and recovery may contain the following activities.

Table 7. Incident management process (adapted from GovCERT.HK)

Incident management process phases	Description of activities in the phase
Containment	This phase aims to contain the incident so that it does not have the capability to extend further into the organization or expose the affected system(s) further. Activities may include: • Assessing the impact of the incident on the system and its data. • Verifying any systems linked to the compromised system through shared network services or trusted relationships. • A critical decision to make is whether to maintain or suspend the operation and service of the compromised system. This decision relies on factors such as the incident type and severity, system requirements, impact on the company's reputation, and predefined goals in the incident handling plan.
Eradication	The eradication phase aims to eliminate or mitigate the root cause of the security incident. Activities may include: • Stopping or terminating all active processes initiated by the attacker. • Removing any files, programs or backdoors created by the attacker, possibly archiving them for investigation purposes before deletion. • Applying patches to identified vulnerabilities across all operating systems, servers, network devices, etc. • Correcting any misconfigurations in system and network settings, such as those in firewalls. • In the event of a malware infection, removing the malware from all infected systems and media. • Updating passwords for all login accounts accessed by the attacker.

Recovery	The objective of this phase is to return the system to its normal functioning. Activities may include: • Assessing the extent of the damage. • Disabling unnecessary services and reinstalling deleted or damaged files, or the entire system, from trusted sources as necessary. • Gradually restoring functions or services in a controlled manner, prioritizing critical or widely used services. • Notifying all relevant parties, such as operators, administrators, senior management, and others involved in escalation procedures, about the resumption of system operation. • Documenting all actions taken for future reference and process development.

According to Knerler et al. (2022), incident responders conduct thorough investigations before acting to accurately assess the required response. Simple incidents might need minimal examination, but more complex situations, like unusual login times hinting at a potential breach, demand in-depth analysis to determine the appropriate course of action. Analyzing security incidents requires cautious interpretation of data without rushing to conclusions, differentiating between facts and speculation, and focusing on understanding the incident rather than immediate attribution. Expanding the SOC's capabilities through collaboration with external experts, like third parties for specialized tasks, can enhance incident management process. (Knerler et al., 2022)

3.3.5 Other processes

In addition to the processes presented earlier, there exist several other processes within a SOC that contribute to its overall operation and effectiveness. However, these processes, while important, can be considered as supporting functions or additional services for some SOC customers. While these processes may play a crucial role in ensuring the properly operating and compliance of the SOC, they are described briefly in this thesis due to their possible auxiliary nature compared to the processes focused on onboarding, data collection, incident detection, analysis, and incident response.

Vulnerability management: This process is related to recognizing, analyzing, confirming and mitigation vulnerabilities in organizations systems and applications. Baek & Kim, 2019, present the following five phases vulnerability management process:

1. **Framing:** Establishes the context and provides a shared perspective on how the organization manages vulnerabilities. Framing guides to identify possible constraints such as financial, legal/regulatory, or technical limitations, and provides a framework for addressing them. Framing also determines the organization's tolerance for vulnerabilities, which serves as the basis for prioritizing and making trade-offs during vulnerability management.

2. **Identification:** This phase consists of assets and vulnerability information. Initially, assets of the organization are identified through the creation of an inventory. Furthermore, assets are categorized and assigned operational value based on criticality to prioritize them. The vulnerabilities are identified by collecting information from sources like Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and vendor disclosures. This phase utilizes both the asset inventory and vulnerability database to identify assets and vulnerabilities impacting the system.

3. **Assessment:** This phase evaluates existing vulnerabilities in assets and their impact on the system, establishing countermeasures accordingly. The assessment results determine whether identified vulnerabilities pose a threat to the system. If so, procedures outlined in the Framing phase are implemented to address them. Evaluation outcomes are reported to management and shared with adjacent or lower-level units.

4. **Remediation:** Addresses vulnerabilities based on their priority determined by risk level and operational impact. Implementation of remediation strategies may be delayed due to factors like availability constraints or budget limitations. Tracking the status of the remediations is paramount to follow that remediations are done in a timely manner.

5. **Verification:** Follow-up audits are done to confirm the remediation of vulnerabilities. Verification is based on the tolerance level defined in the Framing step. If the risk posed by vulnerability remains, additional measures are established through reassessment and verification until complete remediation is achieved. (Baek & Kim, 2019)

Threat hunting: A process aimed at proactively discovering previously unidentified or ongoing threats that have not been remediated within an organization. According to Agarwal et al., 2021, threat hunting is a structured approach designed to uncover the presence of attacker tactics, techniques, and procedures (TTP) in areas undetected by existing detection technologies. It involves six stages: defining purpose and scope, assembling necessary tools, reviewing plans, executing actions, and providing feedback. (Agarwal et al., 2021)

1. **Defining purpose:** The purpose of the threat hunt should align with organizational objectives and how threat hunting contributes to risk reduction. The specific objective outlined may not replace

the task of conducting detailed threat analysis, it can still provide a broad direction for focusing the threat hunt on specific geographic or subsystem areas significant to business goals.

2. **Scope:** The main aim of the stage is identifying specific systems, processes, and entities for investigation. Additionally, it establishes hypotheses or investigative questions regarding the set targets for the threat hunt to achieve the predefined objective.

3. **Assembly:** This stage involves developing a comprehensive data collection and analysis strategy. The threat hunter's approach encompasses both the selection of data sources and the analytical methods, techniques, and frameworks employed to address the formulated hypotheses using the identified data sources outlined in the scope stage.

4. **Reviewing plans:** Is about ensuring that the proposed threat hunt aligns with its objectives. A project manager informs stakeholders about the hunt plan to ensure its successful execution. If the hunt team lacks essential tools, this stage identifies deficiencies and possible solutions are recommended. Furthermore, this stage ensures that the hunt's timeframe includes sufficient data collection scope as a final validation before the execution phase.

5. **Execution:** Stage commences with several iterations of data collection and analysis. Threat hunters utilize research techniques to validate or refute hypotheses formulated during the previous stages. Upon completion of all analyses, the preparation of the hunt report begins towards the end of the execution stage. The final hunt report should focus on the outcomes of the hunting activities and the response rationale.

6. **Feedback:** This stage evaluates the impact of all preceding stages on the threat hunt. Upon completion of the hunt, each level involved is asked several questions, including those interested in the review process. These questions, informed by the strengths and weaknesses identified in previous reviews, aim to guide the organization towards managing future threat hunts more effectively. (Agarwal et al., 2021)

Threat intelligence: Bautista, 2018, defines threat intelligence as '*the ability to gain knowledge about an enterprise and its existing conditions and capabilities in order to determine the possible actions of an adversary when exploiting inherit critical vulnerabilities'.* According to Bautista, 2018, threat intelligence employs various aspects of cyber security, including vulnerability management, security configuration management, incident response, and others, alongside a range of tools. This is done to collect network information through monitoring and reporting. (Bautista, 2018)

The threat intelligence cycle has the following six steps:

1. **Planning and Direction:** This initial phase involves identifying the information needs and establishing a plan to gather the required intelligence. It encompasses the creation of specific information requirements, prioritization, and tasking of collection resources.

2. **Collection:** During this stage, relevant data and information are collected from various sources to meet the predefined requirements. This step ensures that the collection efforts are aligned with the intelligence needs and are efficiently managed.

3. **Processing:** Once the information is collected, it undergoes processing to convert it into a format usable by analysts. This includes organizing the data, mapping it to relevant points, and preparing it for further analysis.

4. **Analysis and Production:** In this critical phase, the processed information is analyzed, evaluated, and integrated to produce finished intelligence products. These products are tailored to the needs of stakeholders, ensuring they are comprehensive, timely, and accurate.

5. **Dissemination:** The intelligence products are then distributed to the appropriate recipients in a manner that facilitates quick understanding and action. Various methods and channels are used to ensure the intelligence reaches those who need it, in the format that is most useful to them.

6. **Utilization:** The ultimate value of intelligence is realized through its application in decision-making and operations. This step emphasizes the importance of using the disseminated intelligence to inform actions and strategies at all organizational levels.
(Bautista, 2018)

These steps form a cycle, highlighting the continuous and iterative nature of intelligence work, where the use of intelligence leads to new requirements and the cycle begins anew.

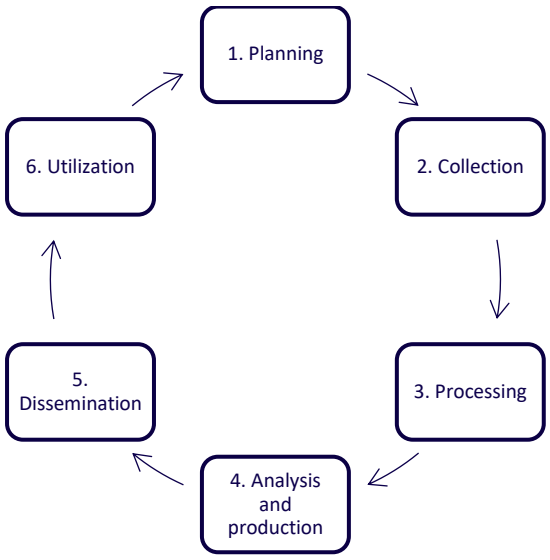

Figure 5. Threat intelligence process cycle (adapted from Bautista, 2018)

Change management: The purpose of the change management process is to evaluate proposed changes to the IT environment. It is often lead by an entity called Change Advisory Board (CAB).

According to Mutemwa et al., that while many organizations view the CAB's primary function as authorizing changes, its true purpose should be to offer guidance on changes. Additionally, the CAB plays a crucial role in assessing risks and mitigation strategies associated with specific changes, as well as potential threats to business continuity. Given the CAB's defined role and responsibilities within an organization, it's imperative that a member of the SOC be included in the CAB. Furthermore, during the implementation and integration of SOC technologies, it's essential that the integration process aligns with the organization's IT environment, a task overseen by the CAB. (Mutemwa et al., 2018)

Mutemwa et al., continue that SOC also has a role in cases where an emergency change needs to be evaluated and implemented to the IT environment as fast as possible. Additionally, certain security recommendations stemming from SOC investigations may necessitate emergency changes to the IT environment. This is where Emergency Change Advisory Board (ECAB) comes into play. It is crucial for a member of the SOC team to participate in the ECAB. These changes should be reviewed and approved by the ECAB to mitigate potential vulnerabilities or prevent further breaches within the organization's IT infrastructure. (Mutemwa et al., 2018)

3.4 Technologies

A SOC typically employs the latest technology, including both software and hardware. In contrast, an organization utilizes a diverse range of technology, which can range from the latest to nearing end-of-life or even legacy systems. Organizations may opt to retain legacy technology for various reasons, including cost considerations where the investment in newer technology does not justify the return on investment or when the technology is no longer manufactured. The challenge lies in integrating these various technologies with the SOC's own technology. (Mutemwa et al., 2018)

Nowadays in SOC technologies such as log management, EDR, SOAR, and others, cloud technology plays a crucial role, either through direct utilization or availability of these technologies in cloud-based models. When integrating cloud technologies, SOCs should consider the possibility of unauthorized tool updates, the location and control of critical security data, legal implications of data storage locations, fluctuating cloud costs, the flexibility to test different tools without long-term commitments, lower barriers for large-scale deployments, and the enhanced flexibility in scaling resources. (Knerler et al., 2022)

It is uncommon for SOCs to entirely avoid cloud usage; instead, the focus is on the degree of reliance on cloud technologies. This dependency ranges from minimal, with automatic updates from the cloud for cyber threat intelligence, to complete, where the SOC's infrastructure is fully cloud-based, including storage, analytics, and automation services. Tools vary in their cloud integration, from on-premises systems receiving updates to entirely cloud-based services, reflecting a spectrum of cloud adoption in SOC operations that can vary inside a single SOC as well. (Knerler et al., 2022)

3.4.1 Log collection

According to Orsos et al., 2022, the foundation of SOC operations lies in the collection, preservation, and analysis of data, which is often log data. Through the examination of gathered log data and employing an appropriate analysis engine, a SOC can assess events as they happen and issue alerts for unusual or suspicious activities. Data collection includes accumulating and storing logs from endpoints, network devices, and other possible SOC components like firewalls, vulnerability scanners, or antivirus programs, and then triggering alerts according to established criteria. (Orsos et al., 2022)

The log collection for the use in organizations cyber defense via SOC is often done via dedicated log management system, a security information and event management (SIEM) tool or increasingly nowadays by utilizing a data lake.

According to Chuvakin, 2016, log management system is meant for exhaustive log collection, aggregation, preservation of unaltered logs, log text analysis, and presentation of the results. The log management systems use of the logs extends broadly across IT, accommodating all conceivable log data uses. SIEM on the other hand encompasses the collection, aggregation, normalization, and retention of logs, alongside context data collection and analysis, presentation, and security-specific workflows and content, with applications centered on information, network, and data security, as well as regulatory compliance. (Chuvakin, 2016)

The key difference between a log management system and a SIEM is dedicated to security and utilizes various IT data for security objectives. Meanwhile, log management is concentrated on the

comprehensive utilization of log data for a broad array of purposes, not limited to but including the security realm. (Chuvakin, 2016)

The concept of data lake has become increasingly popular in recent years, according to Zagan and Danabianu. Data lake can be imagined as a large pool of data, acting as a repository where all incoming data is stored, making it available for later access and usage by various entities within or outside the organization. Essentially it is a modern data storage technology for enabling organizations to store all data in its original, unprocessed form, thereby allowing for the possibility of conducting sophisticated analyses later to extract vital, initially unforeseen insights from the data accumulated at the start of the storage process. (Zagan & Danubianu, 2021)

Table 8. High-level comparison of SIEM vs. log management system vs. data lake

Functionality	Security information and event management (SIEM)	Log management system	Data lake
Log collection	Security relevant logs	All types of logs, including custom logs	All data types in their raw form
Log retention	Processed and normalized log data for limited duration	Preserve both unprocessed and processed log data over extended periods	Preserve both unprocessed and processed log data over extended periods
Reporting	Security-related real-time reporting	Reporting tools suitable for a wide range of purposes, including historical data analysis	Support advanced analytics and reporting

Analysis	Correlating data, scoring threats, and prioritizing events	Comprehensive text analysis and the tagging of log entries	Advanced analysis processes
Alerting and notification	Advanced alerting mechanisms centered on security	Basic alert notifications across all log data	Extensive data analysis capabilities can support anomaly detection and alert generation
Other features	Incident management and analyses of various security-related data	High scalability for broader data handling	High scalability and security for stored data

Adapted from Chuvakin, 2016, and Zagan & Danubianu, 2021

SIEM and log management systems offer two types of log collection techniques. These are agentless methods where logs are either directly sent to or fetched by the server, and agent-based methods where a client-side agent gathers and forwards logs to the server, handling filtering and conversion in the process. (Orsos et al., 2022) & (Chuvakin, 2016)

In data lakes the data collection methods vary between different data lake architecture models. There can be from two-layered data lake structures to complex models incorporating zones and layers designed for specific data handling tasks. These architectures facilitate the collection of heterogeneous data, including high-velocity and semi structured data from IoT devices and APIs, supporting advanced data processing techniques. By and large, data lakes offer flexibility in storing, processing, and providing access to vast volumes of raw and processed data. (Hlupic et al., 2022)

3.4.2 Security information and event management

According to Podzins & Romanovs, 2019, key to effectiveness with security information and event management or SIEM product lies in collecting only specific log sources into it. This is because some log sources, or log types, may be irrelevant or merely duplicate information and may not assist in detecting security incidents. As SIEM software licensing can depend on the amount of log

data processed, and considering the high costs associated with SIEM solutions, it is advantageous to limit the volume of logs reviewed. (Podzins & Romanovs, 2019)

According to Knerler et al., SIEMs have demonstrated their worth in numerous enterprise SOCs since their availability from early 2000s. However, some SOCs find it challenging to fully benefit from SIEM because of its complexity and the resource-intensive nature of writing and maintaining effective correlation rules. (Knerler et al., 2022)

Podzins & Romanovs point that a common mistake made by organizations is to include as many log sources as possible to enhance potential coverage of the SIEM. However, this approach can overload the SIEM with an excessive number of rules to process and possibly generating many false positives, thereby consuming valuable employee time, and rendering both the SIEM system and the SOC operations less effective. (Podzins & Romanovs, 2019)

According to Neil, 2018, SIEMs key features include:

- **Aggregation:** Consolidating logs and data from different sources into one repository.
- **Event Correlation:** Linking related events across systems to identify potential threats, using event de-duplication to log unique events once.
- **WORM Drive Backup:** Securely backing up logs on a WORM (write-once, read-many) drive to prevent tampering.
- **Automated Alerting:** Deploying agents on devices for immediate notification of critical events.
- **Time Synchronization:** Utilizing precise time sources for accurate event timing and organization.
  (Neil, 2018)

According to Knerler et al., despite some deviations, modern SIEM systems share common features and components, particularly in data acquisition and collection. This function is typically handled by an agent or collector, which can be positioned directly on the monitored host—accessing logs via local APIs or file systems—or remotely, either pulling data from devices or receiving data pushed to it. All SIEM architectures require some form of agent for data ingestion, whether located on the host, a nearby system, an appliance, through an SIEM API, or cloud based as a SaaS feature. Typically leading SIEMs provide various deployment options. (Knerler et al., 2022)

Upon receiving log files, SIEM system component normalizes and converts them into a format the system can analyze, applying predefined rules and queries. Different technology vendors SIEM platforms utilize their own approaches to analyze through large volumes of logs, leveraging rule sets and historical comparisons. Recurring patterns, rather than isolated events, often trigger alerts in the SIEMs. Detected incidents are prioritized and presented on the SIEM dashboard, leading to differentiated features among different technology vendors SIEM products. These can include automated responses, notifications, and report generation for management and key performance indicator evaluation. (Podzins & Romanovs, 2019)

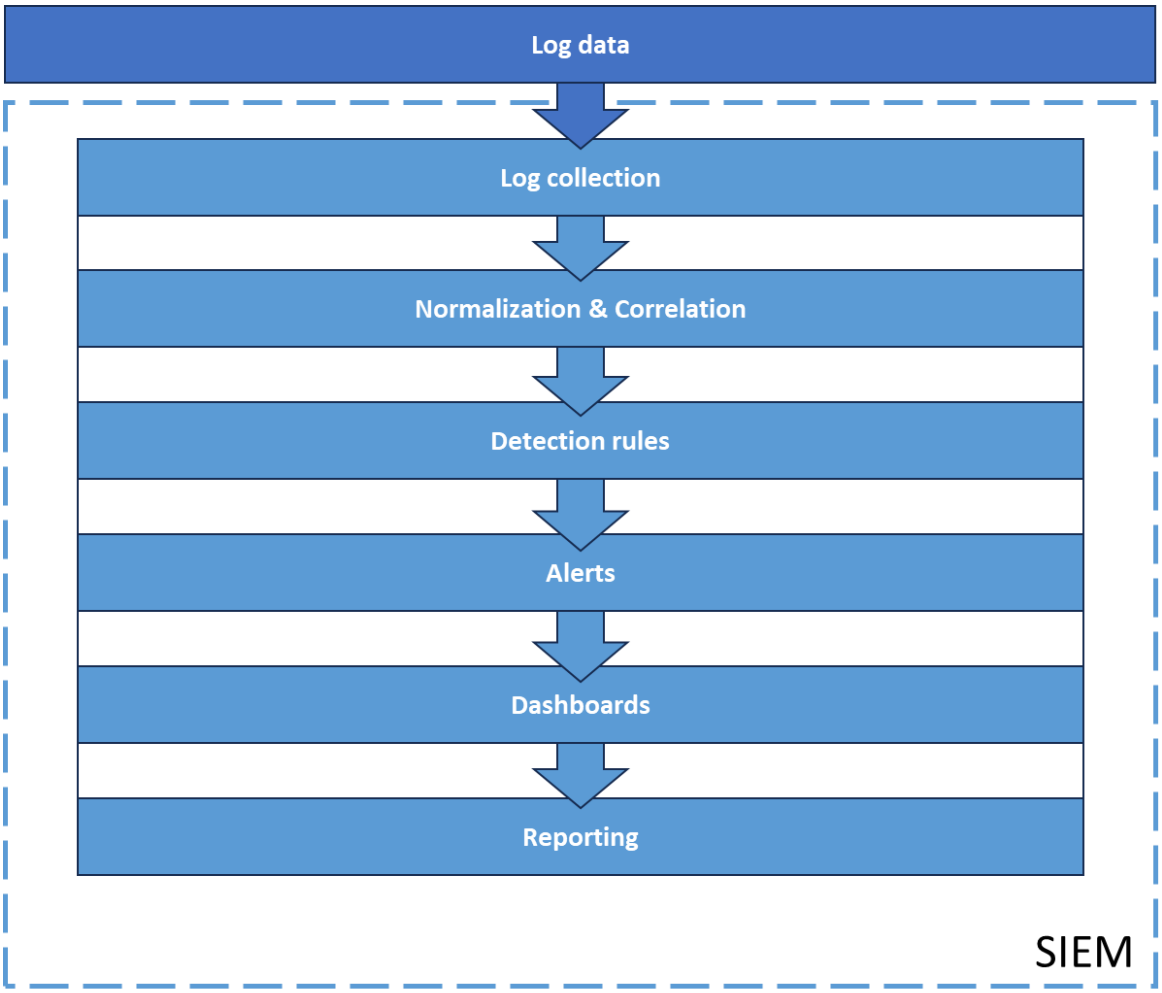

Figure 6. Typical SIEM components (adapted from Podzins and Romanovs, 2019)

3.4.3 Security orchestration, automation, and response

According to Knerler et al., 2022, security orchestration, automation, and response, or SOAR, solutions offer tools and functionalities that streamline and automate routine SOC processes, allowing security teams to efficiently handle repetitive tasks. While SOAR is recognized as a distinct category, it shares many objectives with case management systems and SIEMs. (Knerler et al., 2022)

SIEM systems face a challenge in effectively analyzing the vast amounts of data they collect, often producing reports that are not directly actionable, are difficult to understand, and contain excessive irrelevant information. SOAR emerges as a solution by automating processes through playbooks, streamlining alert identification, and minimizing manual labor. It prioritizes integrating various technological solutions and technologies to achieve security objectives more efficiently. (Sridharan & Kanchana, 2022)

Sridharan & Kanchana argue that SOAR, which was conceptualized by Gartner, aims to integrate functionalities from three distinct security-focused software capabilities: security operations, threat and vulnerability management (orchestration), incident response and security operations automation (response). This integration is designed to decrease human error and oversight in alerts, thereby enhancing the efficiency of responses to vulnerabilities or threats. SOAR thus plays in together with the objective of SIEM, which is to gather all security related information to a single pane of glass, allowing to detect patterns and trends. (Sridharan & Kanchana, 2022)

According to Knerler et al., 2022, by utilizing SOAR, a SOC can:

- Consolidate incident reports from various sources into a unified interface for easier alert triage and management.
- Enhance and rank alerts by incorporating threat intelligence and information about the entities involved.
- Trigger automated actions in response to alerts, such as analyzing suspicious files, retrieving vulnerability scan results, or accessing relevant employee information.
- Conduct common searches within log databases.
- Facilitate standard communications with stakeholders, querying about the legitimacy or expectation of certain activities.
- Implement automatic countermeasures, including cutting off network access or deactivating accounts.

(Knerler et al., 2022)

3.4.4 Endpoint detection and response

Introduced in 2013, Endpoint Detection and Response (EDR), also recognized as Endpoint Threat Detection and Response (ETDR), represents a category of endpoint security technology that operates independently of network security mechanisms. EDR systems are designed to collect data from endpoints, which is then centralized for analysis and storage. These systems dynamically associate and scrutinize events, binaries, etc., to identify and analyze anomalous activities on monitored servers, thereby enhancing the operational efficiency of SOCs through improved detection and notification of cyber threats to both clients and incident response teams. (Arfeen et al., 2021)

EDR technologies have advanced host monitoring capabilities providing comprehensive analysis of operating system data to detect adversaries. Furthermore, EDR offers an improved framework for detecting and responding to threats, covering every phase of the cyber-attack lifecycle. This holistic approach ensures that organizations can more effectively anticipate, identify, and neutralize threats before they can cause significant damage. (Knerler et al., 2022)

Implemented via endpoint agents or sensors, EDR solutions aggregate security data for advanced analysis at a centralized location. EDR solutions process to recognize malicious patterns and detect malware, while prompting alerts for mitigation actions or further analysis. Correspondingly, incident response teams must act against the attack kill chain with the steps—preparation, containment, eradication, and recovery—to address security incidents effectively. EDR platforms support these efforts by providing capabilities for detection, reporting, quarantining, and neutralizing threats throughout every phase of an attack cycle, thereby enhancing an organization's incident response framework. (Arfeen et al., 2021)

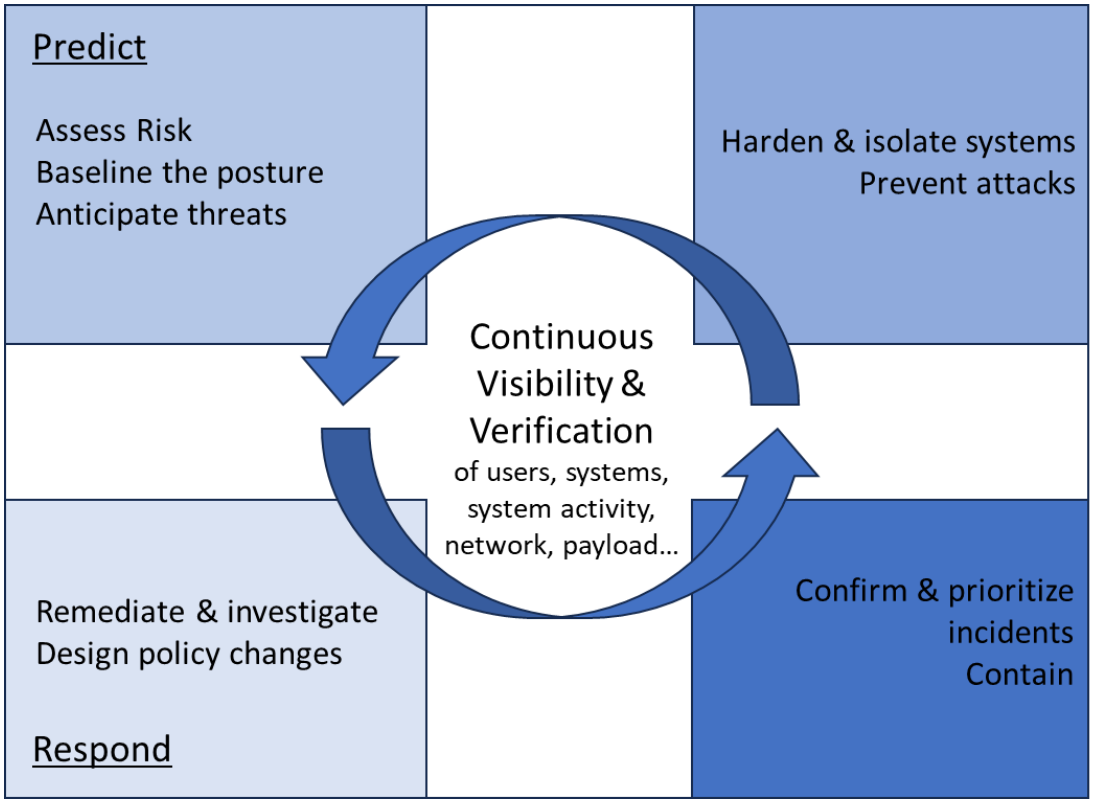

Figure 7. EDR functionalities (adapted from Firstbrook et al., 2017)

3.4.5 Other technologies

As with the processes in chapter 4.2, there exist several other technologies which are utilized by SOCs in their day-to-day operations. While some of these technologies are among the primary technologies in some SOCs, they are described briefly in this thesis due to their possible auxiliary nature compared to the previously mentioned technologies.

Threat intelligence platform: Organizations have increasingly adopted threat intelligence platforms (TIPs) to facilitate the sharing and collaborative analysis of cybersecurity information. These platforms streamline the exchange and validation of data, contributing to process automation. (Dannana et al., 2022)

Even large governmental entities such as the United States of America's Department of Homeland Security enhances its threat intelligence capabilities through partnerships with the threat intelligence community. Information sharing and collaboration regarding cyber threat intelligence can be regarded as a standard practice. There is a variety of open-source threat intelligence tools,

ranging from commercial to free solutions. Organizations can begin integrating threat intelligence by subscribing to threat intelligence (TI) feeds. Incorporating threat intelligence offers the benefit of tailoring data against specific adversaries. For instance, a financial institution would benefit from threat intelligence on adversaries targeting the financial sector, rather than receiving irrelevant alerts from other sectors, such as education. Understanding the assets the organization is protecting helps to focus on the relevant threat actors, with threat intelligence providing critical insights to detect these threats. (Diogenes & Ozkaya, 2018)

Dandurand and Serrano, 2013, outline three primary objectives for threat intelligence platforms:

1. facilitate the sharing of cyber threat intelligence.
2. automate the collection, storage, and processing of cyber threat data, converting it into actionable intelligence and sharing it efficiently.
3. foster collaborative efforts among various stakeholders in addressing cyber threats.

(Dandurand & Serrano, 2013)

Understanding your adversaries enables better protective measures for your assets. However, threat intelligence can be more than an IT security tool. It can guide organizational defense strategies, inform security investment decisions for managers, and support in executive briefings to the organization’s management. Threat intelligence's insights can have a broad applicability across various organizational domains as a strategic decision-making asset. (Diogenes & Ozkaya, 2018)

Vulnerability scanner: According to Neil, 2018, vulnerability scanner operates as a passive tool, that identifies system vulnerabilities or weaknesses by scanning the information environment it has been set to scan. Such vulnerabilities and weaknesses could range from outdated operating system patches and antivirus software to the existence of a sole administrator account, highlighting areas that may compromise organization’s cyber security. Vulnerability scans come in two varieties: credentialed and non-credentialed. Credentialed scanners operate with administrator privileges, enabling them to uncover vulnerabilities, audit files, and review permissions comprehensively. Non-credentialed scanners, on the other hand, function with restricted permissions, focusing primarily on identifying missing patches by scanning hosts, offering a more surface-level assessment. (Neil, 2018)

The findings of a vulnerability scan can include:

- Appropriate permissions have been set for users and applications.
- Identification of services which should not be authorized to be run.
- Unnecessary applications.
- Missing patches.
- Misconfigurations such as, incorrect flow of data, unnecessary services, improper firewall configurations, unnecessary user rights.
- Baseline check to recognize any unauthorized applications.
- Some vulnerability scanners can also test the source code of application to recognize vulnerabilities before they are deployed.
  (Neil, 2018)

It is important to note that the findings can include false positives, where the scanner incorrectly identifies a non-existent vulnerability, and false negatives, which are more critical because the scanner fails to detect an actual vulnerability, such as a zero-day exploit that remains undetectable. (Neil, 2018)

3.5 Summary of People, Processes and Technology for SOCs

As it was visible from this non-exhaustive review of people, processes, and technologies, SOCs are multifaceted entities that do not have a strict academic definition of what they would or would not contain or what their operational capabilities would be. The attempt of this chapter was to capture what themes would rise from academic literature as the overarching qualities in people, processes, and technologies for a SOC. The author felt that this was a necessary effort to try and capture what components are usually overarching in all the different SOC compositions that are out there.

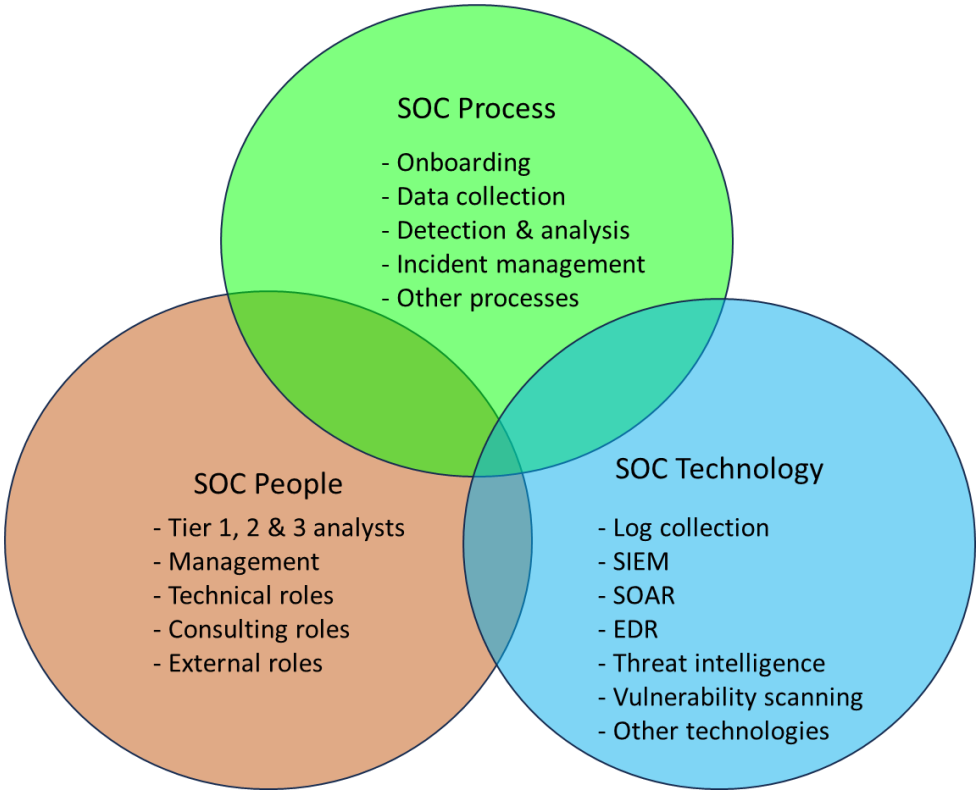

Figure 8. Brief summary of PPT qualities of a SOC

4 Continous Threat Exposure Management by Gartner

According to the 2022 Gartner publication Implement a Continuous Threat Exposure Management (CTEM) Program, organizations are facing changing technological environments and business practices such as Software-as-a-Service, operational technology, and Internet of Things, which requires organizations to update their security programs to safeguard these new IT assets. Also, practices such as remote work and increasing number of information interfaces with suppliers require organizations to rethink how they should protect their IT environments and operations. Gartner continues that traditional vulnerability management approaches are not anymore enough to adequately respond to the threats faced by the multi-faceted IT ecosystem that many modern organizations maintain. Patching every recognized vulnerability was never a possibility in the past either but, according to Gartner, more advanced risk-based vulnerability management efforts will probably not be enough either as potential attack surfaces to organizations have expanded and become more varied. (Gartner, 2022a)

Gartner presents continuous threat exposure management or CTEM as the approach that can respond *"…in an age where organizations can't fix everything, nor can they be completely sure what vulnerability remediation can be safely postponed"* and continue to define it as *"…CTEM programme is an integrated, iterative approach to prioritizing potential treatments and continually refining security posture improvements."* (Gartner, 2022a)

Gartner (2023b) publication Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management defines CTEM as *"an umbrella program for forward-looking and sustainable approaches to exposure reduction."* The publication states CTEM is involving business functions in identifying the organizations crown jewels, or the most valuable units or assets of an organization, that need to be protected against cyber adversaries or disruptions. Implementing a CTEM program can be thought as coordinating the cyber risk management efforts to not just defend against generic cyber threats but also tailoring the organization's response to protect the most critical aspects of its business. (Gartner, 2023b)

The concrete goal of a CTEM program is to provide clear input for enhancing the organization's security that both business leaders can understand, and architectural teams can implement. The controlling factor in this work is the organization's risk appetite that guides the remediation actions between fixing and mitigating issues or working with a combination of these two methods. (Gartner, 2022a)

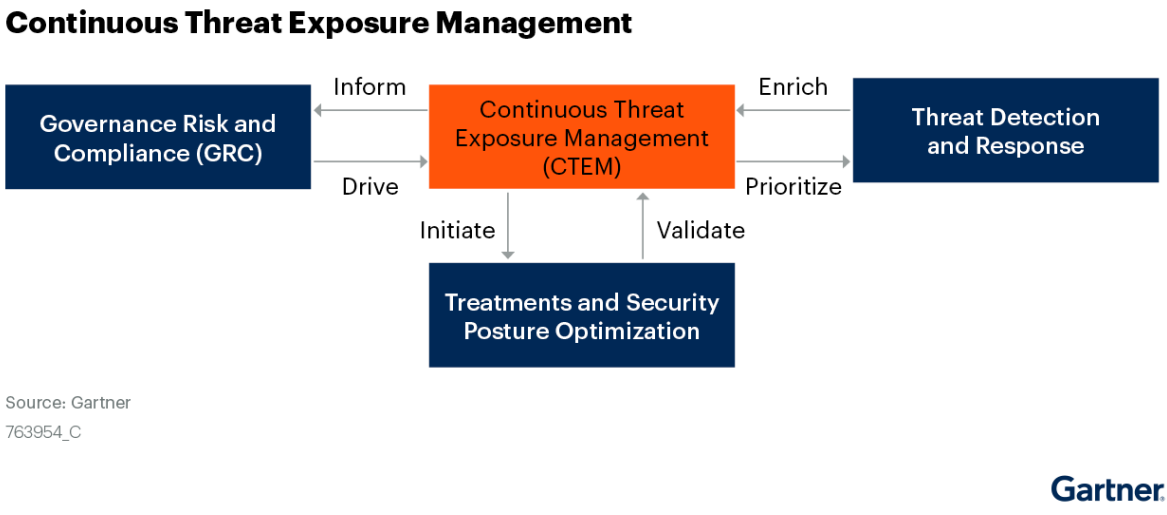

Figure 9. Continous Threat Exposure Management by Gartner (2022a)

As the above figure illustrates, the CTEM program does not operate in isolation from other security efforts in the organization. The organization's governance, risk and compliance (GRC) function provides the CTEM program with the strategic level input to help focus the CTEM efforts. These can include for example, engaging with the CTEM to follow the relevant laws, regulations, and industry standards for that organization. The threat detection and response (TDR), which is mostly associated in what SOC does, provides the CTEM with information what are the current threats facing the organization, or the industry. Treatments and Security Posture Optimization are validating the addressed security vulnerabilities and the enhanced overall security measures. By and large, a successful CTEM program requires that clear communication protocols, understandable information content and formal processes for cross-team collaboration are established. As it was earlier stated, the input needs to be something that both business leaders can understand, and architectural teams can implement. (Gartner, 2022a)

Gartner (2022a) also points that even though CTEM program might utilize automated technologies, overreliance on just accumulating assessment reports or investing in a single, all-encompassing platform that claims to handle everything has its perils. Overreliance on tools like this can create fatigue on alert handling, where alerts can be overlooked by teams due to the vast amount of the alerts. Reliance on what only tools produce can create situations where the teams lack the business context knowledge and knowledge of successful remediations of vulnerabilities or posture improvements. Reliance on tools and their automation to detect, respond and contain cyberattacks can also lead to challenges in business accountability. (Gartner, 2022a) An example of this could be a situation where a team who is using and maintaining an asset might think that the vulnerability or posture improvement is resolved by the tool, or the team responsible for the tool, will provide the remediation. The team responsible for the tool might assume that the team owning the asset will assume responsibility for remediation and workflow initiation when they are informed about the finding.

"CTEM might suggest "treatments," such as technical mitigations, but "remediation" implies that the suggested course of action must also pass through the standard processes for risk acceptance, as well as operational viability." (Gartner, 2022a)

On the 2024 Strategic Roadmap for Managing Threat Exposure publication, Gartner (2023c) stated that it believes that the exposure management tactics and techniques will take over the vulnerability management practices that have been the choice for many organizations. According to the publication, the organizations that recognize the increasingly complex IT ecosystem will adapt their tools and tactics to follow assessment processes that provide more continuous information about the cyber threats, on the of the processes being CTEM. (Gartner, 2023c)

The rising interest towards CTEM seems to be true at least in Gartner's viewership, as according to Gartner Peer Community survey poll, 29% of responders stated that their organization has a CTEM program, with 61% either developing or considering developing one. At the time of the writing the poll had 390 participants. (Gartner, 2024a)

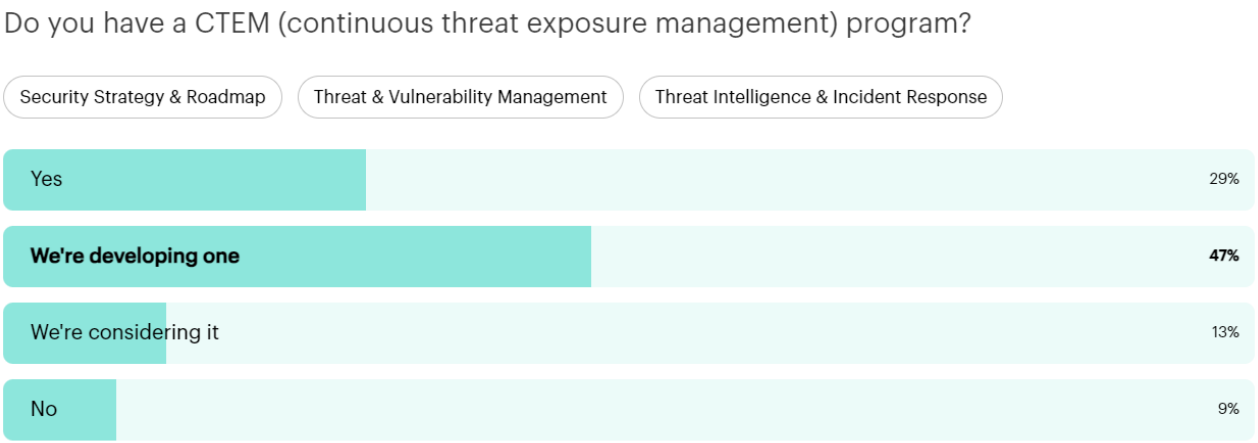

Figure 10. Do you have a CTEM Program? Gartner Peer Community Poll (2024a)

Gartner (2023b) states that often many technologies and projects that would benefit the organization's CTEM program are already implemented by the organization. The issue is that these are implemented so that the results are not cross-referenced and combined to get a 'single pane of glass' type of view of the cyber threats or the remediation situation for them. (Gartner, 2023b)

4.1 The five steps of CTEM cycle

A CTEM program consists of five steps where different activities take place to contribute to the program. The repetition of these steps in each iteration of the CTEM program helps to continuously improve and refine the organization's security posture over time. How CTEM program distinguishes itself is that it sets itself to provide answer to the questions of “why” and “how”. (Gartner, 2022a) This can be understood that CTEM tries to answer "why" these vulnerabilities or discoveries matter in the context of the organization's threat landscape and "how" they should be prioritized and addressed to align with the organization's security strategy and business goals. On the other hand, the traditional vulnerability management program can be seen to answer to the questions “what" vulnerabilities exist and "where" they are located within the organization's IT infrastructure.

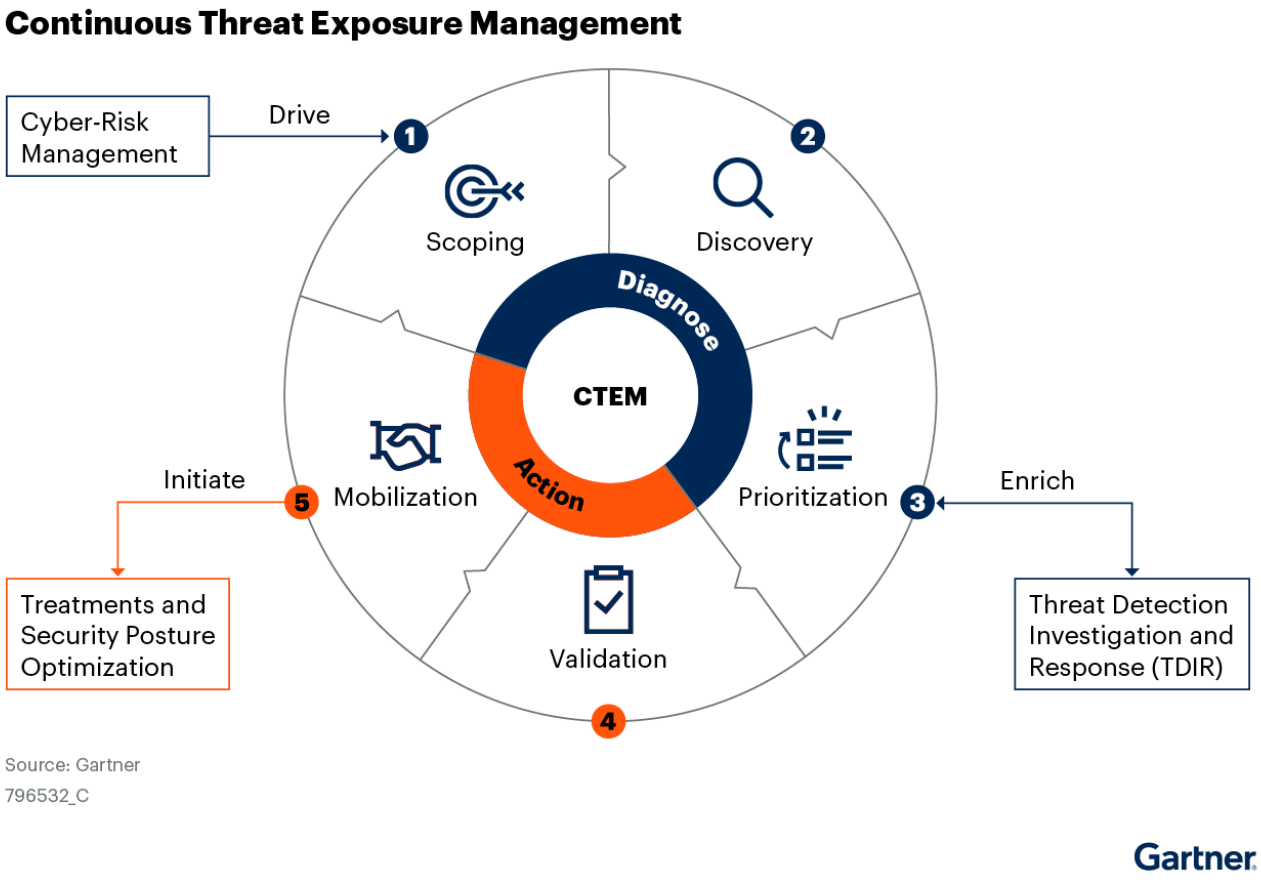

Figure 11. Continuous Threat Exposure Management by Gartner (2023b)

According to Gartner (2022a), a CTEM program serves as the initial action taken for recognizing cyber threats and organizing actions to resolve them in organizations. CTEM program emphasizes the necessity for cooperation between different teams within an organization, including distribution of duties and responsibilities. The cooperation becomes especially paramount when it comes to assets or work phases where the responsibilities can be shared. As an example, while a security operations team focuses on the identification and follow-up of exposures, the architecture teams can be responsible for the practical side of remediation. A security operation team can also perform the validation of the remediation after the architecture team's work. (Gartner, 2022a)

CTEM program tries to establish structured and repeatable workflow. The repeatable nature of the workflow means that the process can be conducted systematically and consistently across different instances of threat exposure, leading to a more organized and effective management of cybersecurity risks. (Gartner, 2022a)

CTEM is a repetitive or cyclical process, meaning it goes through its stages repeatedly over time. CTEM process is influenced by external and internal factors, or triggers, to the organization. Examples of these can be start of new business projects, change in risk appetite or changes in current controls or personnel. A change in these factors do not always require starting the CTEM cycle from its initial stage. Depending on the situation, an organization might jump into the CTEM process at a different step that is more relevant to the specific trigger or event. (Gartner, 2022a)

As presented in the Figure 10, the stages of CTEM are *Scoping, Discovery, Prioritization, Validation* and *Mobilization*. These stages are presented in more detail in the following sub-chapters starting from 4.1.1 until 4.1.5. The recognized required capabilities for that CTEM program step, following the People, Process and Technology framework, **will be bolded in the subchapters**, and presented in a table at the end of each sub-chapter. Each of recognized capabilities will be categorized as per the People, Process and Technology framework. In case some capabilities are mentioned several times in the text they will be only bolded and mentioned in the table once.

4.1.1 Scoping

The scoping step is meant to ensure that the focus of the CTEM program remains on aspects that are critical to the organization's needs and goals. This means before looking for vulnerabilities or threats, the organization **defines what areas, assets, or processes are most important to protect based on their value to the business**. (Gartner, 2022a) As it was stated earlier, modern organizations have multi-faceted IT ecosystem consisting of servers, end-user devices and applications. The current IT ecosystem also extends to that might not have in the past considered to be part of the cybersecurity domain.

Gartner (2023c) instructs that in the beginning of scoping, organization needs to **consider how the risk would affect organizations crown jewels and how the business evaluates this risk**. What business-based events will likely to be important in the foreseeable future, who own the associated processes and what are the most critical or exposed IT assets associated with those processes are some of the questions that need to be asked during scoping phase. It is also paramount to understand where these assets are, **who are their owners and who are ultimately accountable for making risk decisions and changes regarding these assets**. (Gartner, 2023c)

Because of this, Gartner (2023c) states that the CTEM program scope should also be reached to assets that the organization does not own and control. Examples of these can include Software-as-a-Service, code repositories, organization’s social media, third-party services, and supply chain relationships. CTEM program can have several different scopes running at the same time. Gartner states that scoping should be considered more as parameters for reporting, not as the coverage of the whole CTEM program. (Gartner, 2023c)

Unlike traditional approaches that might focus predominantly on diagnosing security issues or vulnerabilities, CTEM aims to create actionable output. This transformation requires a clear understanding of what the organization aims to achieve through its CTEM program and the scoping step is important to be able to answer the “why” and “how” questions introduced earlier. According to Gartner, it can be argued that CTEM program goes even further than managing the security vulnerabilities and exposures internally, and **taking the cyber adversaries mindset** to see and validate the “why” and “how” the adversaries would target these. (Gartner, 2022a)

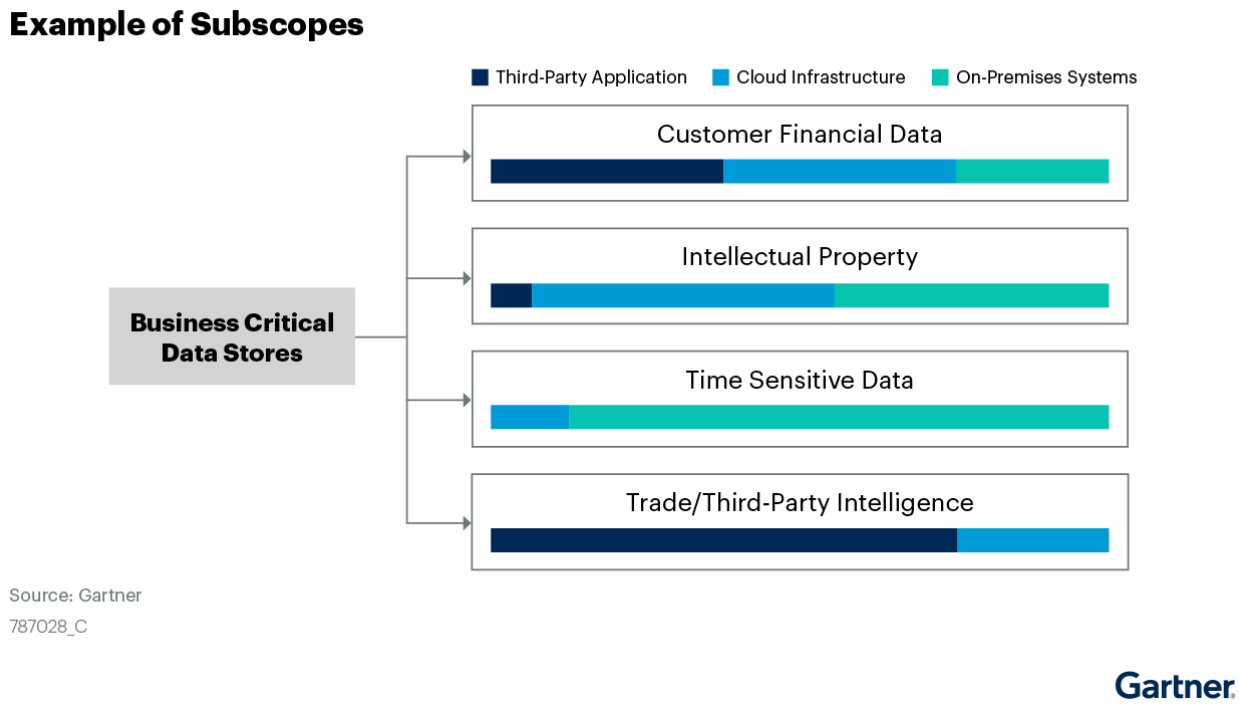

Figure 12. Example of Subscopes by Gartner (2023c)

Gartner (2023c) recommends that scopes are defined as they are related to the organization, meaning that rather than broad and technical categories like "all internet-facing assets," scopes should be defined in terms of their direct relevance to the organization's operations and objectives, example being given as "revenue-driving, web-facing applications." Also, Gartner points out that an organization can operate multiple scopes simultaneously under CTEM program without a predefined cap on their number. An overarching "master scope" can be created that is easily understandable and relevant to business stakeholders, under which "subscopes" can be defined that focus on more specific technical aspects. (Gartner, 2023c)

Gartner (2022a) lists following the tools & techniques that are included in this step of the CTEM: monitoring the **external attack surface**, **Software as a Service (SaaS) applications security posture**, **digital risk protection**, and utilizing **dark and deep web sources** to identify potential threats. (Gartner, 2022a)

Table 9. Scoping capabilities

Mentioned capability	PPT category
who are their (assets) owners and who are ultimately accountable for making risk decisions and changes regarding these assets	People
taking the cyber adversaries mindset	People
defines what areas, assets, or processes are most important to protect based on their value to the business	Process
consider how the risk would affect organizations crown jewels and how the business evaluates this risk	Process
External attack surface -tool	Technology
SaaS security posture -tool	Technology
Digital risk protection -tool	Technology
Dark and deep web sources	Technology

4.1.2 Discovery

Discovery process involves **identifying the assets within the scoped areas and assessing their risk profiles**, which includes understanding the types of threats and vulnerabilities each asset may be exposed to. The priority for discovery step should be on those areas of the business deemed most critical by the scoping process, but there should be also flexibility in approach based on the organization's needs and emerging threats. (Gartner, 2022a) The flexibility is needed in situations where a significant cyber threat emerges globally or locally that requires a new evaluation of priorities or when organization does changes that have an immediate effect to its operations. There are however reasons to not to change the initial scope which we will get into later in this chapter.

According to Gartner (2022a) discovery is not only about **finding vulnerabilities** in software or hardware, but it also includes **identifying misconfigurations in assets and security controls**. Beyond technical vulnerabilities and misconfigurations, discovery efforts related to CTEM should also

identify other types of weaknesses, such as the presence of fake or unauthorized assets, sometimes called shadow IT, within the organization's inventory, **or poor results to phishing tests**, which indicate vulnerabilities in human behavior and organizational processes. (Gartner, 2022a)

Gartner states that the traditional approaches to scanning and vulnerability management are not enough by themselves to respond to the current need of organizations. Traditional scanning and discovery methods, such as **application, discovery, and host scanning**, are usually limited to the organization's directly managed IT infrastructure. These scans are then less effective at identifying vulnerabilities in the third-party services or platforms that the organization utilizes. This leaves potential attack vectors unaddressed because these methods do not account for the full IT ecosystem that organizations operate within today. Examples of these were the **Software-as-a-Services, code repositories, organization's social media, third-party services** etc. (Gartner, 2023c)

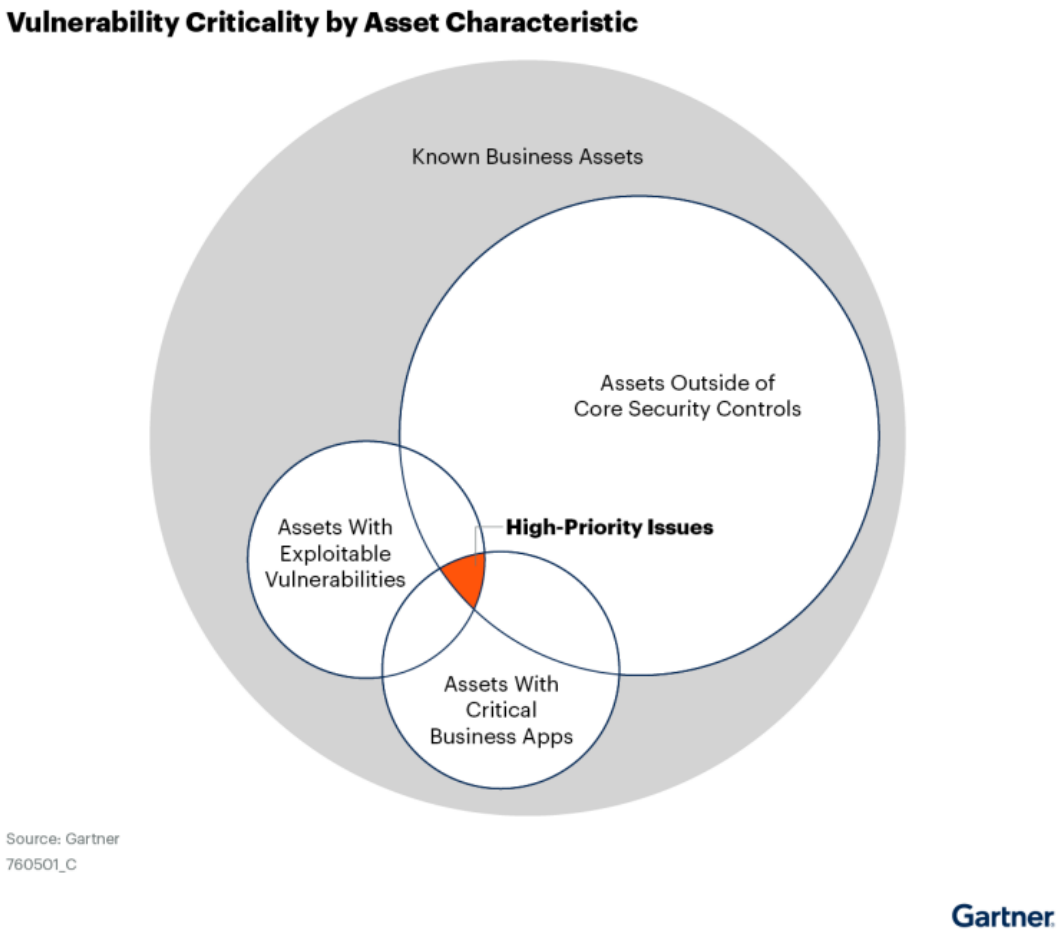

Figure 13. Vulnerability Criticality by Asset Characteristic by Gartner (2023c)

It is likely that during discovery step, assets, vulnerabilities, misconfigurations, and other risks that extend beyond the originally defined scope are identified. This expansion can occur as both known and previously unrecognized assets and their associated vulnerabilities are discovered, along with various types of risks and misconfigurations that were not initially considered. (Gartner, 2022a)

When this happens, Gartner (2024b) argues against adjusting the scope or restarting the current CTEM cycle. Since CTEM is designed to be a continuous and potentially parallel process, incorporating these new findings into the current cycle could delay the next steps of the cycle. Gartner advises that instead of reshaping the ongoing cycle, **newly identified assets and vulnerabilities should be noted** and included in the scoping phase of subsequent CTEM cycles. This approach is done to ensure that the program remains dynamic and responsive to new information without disrupting ongoing activities. (Gartner, 2024b)

Gartner (2023c) also points out that tools might flag issues that are either not prioritized or are assigned a low priority level. The reason is that these tools and methods typically rely on analyzing metadata or conducting non-invasive scanning techniques, which can identify potential vulnerabilities but might not provide enough context or detail to accurately assess the severity or immediacy of the threat they pose. Essentially, while these tools are effective at uncovering a broad range of issues, their initial assessments regarding the priority of these findings may not always be reliable. (Gartner, 2023c)

Table 10. Discovery capabilities

Mentioned capability	PPT category
identify other types of weaknesses, such as the presence of fake or unauthorized assets or poor results to phishing tests	People
identifying the assets within the scoped areas and assessing their risk profiles	Process
finding vulnerabilities & identifying misconfigurations in assets and security controls	Process
newly identified assets and vulnerabilities should be noted	Process
application, discovery, and host scanning	Technology

Software-as-a-Services, code repositories, organization's social media, third-party services	Technology

4.1.3 Prioritization

The purpose of the prioritization is to filter the results received from the previous step and direct the focus and the efforts on the ones that make sense for the business or security of the organization. Organizations should **identify their high-value assets**, those critical to business operations and containing significant business value, to determine the focus of their treatment efforts. This involves **assessing whether adequate security controls are already in place** to protect these assets and **evaluating the likelihood that these assets could be targeted and exploited by adversaries**. (Gartner, 2022a)

Gartner (2023c) argues that type of the discovered threat or exposure and the rated severity of it are not enough to do a comprehensive prioritization. Using frameworks such as MITRE ATT&CK and common vulnerability scoring system (CVSS) is useful but when they are used in isolation, these frameworks and scoring systems may not account for the unique impact a specific vulnerability or exposure could have on an individual organization. (Gartner, 2023c) An example of this would be cases where an organization does not consider if the vulnerable or exposed asset is located in a location that makes the exploitation of it harder, the possible other security controls the asset has in place, the value of the asset to the organization's operations, or if the vulnerable functionality of the asset is even enabled or used.

According to Gartner (2022a), by considering these factors, organizations can strategically allocate their resources and efforts towards mitigating the most significant risks, ensuring that the most critical assets are protected in line with the organization's risk tolerance and security goals:

- Urgency
- Severity
- Availability of compensating controls
- Risk appetite
  Level of risk posed to the organization. (Gartner, 2022a)

According to 2024 Strategic Roadmap for Managing Threat Exposure publication by Gartner (2023c), additional information that can add context and relevance to the prioritization process includes **threat intelligence data related to vulnerability or exposure** in terms of availability of exploits or the data regarding the threat actor interest toward that exploit. Other suggested enrichment methods include the **usage of benchmarks to similar organizations and using historical data on past security breaches** to help understand the likelihood and potential impact of certain vulnerabilities within the organization's industry context. The aim of these efforts is to make these more understandable and relatable to business owners to help them make investment decisions to the exposures that really matter. (Gartner, 2023c)

However, as everything cannot be a priority, a CTEM program should also **include the conclusion why something was deprioritized** based on the above-mentioned factors. This process ensures that protecting essential business operations is the main focus of the CTEM program, while still being able to quickly respond to unexpected or severe threats like zero-day vulnerabilities. However, as Gartner points out in the below statement, as per the CTEM program even prioritized list of remediation activities might require more effort before they are executed. (Gartner, 2022a)

"Even a clearly articulated list of prioritized treatments (e.g., patches, signatures, configuration changes) might not be enough to trigger the required collaborative approach to remediating the highlighted issues." (Gartner, 2022a)

Table 11. Prioritization capabilities

Mentioned capability	PPT category
identify their high-value assets	People
assessing whether adequate security controls are already in place & evaluating the likelihood that these assets could be targeted and exploited by adversaries	Process
usage of benchmarks to similar organizations and using historical data on past security breaches	Process
include the conclusion why something was deprioritized	Process
threat intelligence data related to vulnerability or exposure	Technology

4.1.4 Validation

In validation the **potential attack** the cyber adversaries could do **against the detected vulnerability or exposure is assessed by the organization**. Part of the validation process is also the **assessment whether the exploitation of the exposure would be detected by the monitoring capabilities**. This process often involves conducting controlled simulations of attacker techniques, or red team operations, within the organization's actual operational environment to test defenses. (Gartner, 2022a)

Organizations will find themselves facing many issues deemed as priorities. Validation helps to distinguish between vulnerabilities that pose a real and immediate threat from those that, despite being identified, may not be as critical in practice or may not be exploitable due to existing controls or mitigations. Without validation, organizations may waste resources addressing vulnerabilities that do not significantly impact their security posture, leaving them with an overwhelming volume of supposed priorities. (Gartner, 2023c)

According to Gartner (2022a), following objectives should be achieved in this step:

- Confirming that identified and prioritized vulnerabilities could realistically be exploited by attackers, ensuring mitigation efforts are targeted at genuine threats.
- **Analyzing potential attack paths from initial vulnerabilities to critical business assets**, to understand the full extent of possible damage and prioritize the protection of key assets.
- Evaluating whether the organization's **response and remediation processes are quick and effective enough to address vulnerabilities** without negatively impacting business operations. (Gartner, 2022a)

Automated validation tools, such as **Breach and Attack Simulation (BAS) systems** and **automated penetration testing tools**, can help to evaluate if identified vulnerabilities are exploitable, thereby confirming their practical threat level. These tools also conduct in-depth analyses to trace potential attack paths through the network to critical assets. Additionally, they assess the organization's response and remediation efficiency by testing how quickly and effectively it can address and mitigate these simulated threats. (Gartner, 2023c)

Validation also includes the **evaluation of the proposed treatments** for mitigating the vulnerabilities or exposures. This evaluation looks at two main aspects: the effectiveness of these treatments in enhancing security and their practicality within the organization's operational and structural context. This ensures that the security measures are not only theoretically possible against the threats but are also viable and implementable within the specific organizational environment. (Gartner, 2022a)

Also, it is important to **validate the response process** to see that the organization is adequately prepared to handle real security incidents. However, validation of human responses and procedural effectiveness, cannot be fully automated. In those cases, **red team exercises or** contracting **Penetration Testing as a Service (PTaaS)** can be employed **to simulate realistic attack scenarios**. Regularly conducting these exercises help identify weaknesses in security processes, enhance organizations response efficiency and provide feedback for improvement. (Gartner, 2023c)

Table 12. Validation capabilities

Mentioned capability	PPT category
evaluation of the proposed treatments	People
validate the response process to see that the organization is adequately prepared to handle real security incidents.	People
potential attack the cyber adversaries could do against the detected vulnerability or exposure is assessed by the organization	Process
assessment whether the exploitation of the exposure would be detected by the monitoring capabilities	Process
Analyzing potential attack paths from initial vulnerabilities to critical business assets	Process
Evaluating whether the organization's response and remediation processes are quick and effective enough to address vulnerabilities	Process
red team exercises or contracting Penetration Testing as a Service (PTaaS) can be employed to simulate realistic attack scenarios.	Process
Breach and Attack Simulation (BAS) systems and automated penetration testing tools	Technology

4.1.5 Mobilization

Gartner's Top Strategic Technology Trends in China for 2024: Continuous Threat Exposure Management publication states that mobilization transitions the CTEM program approach from isolated tasks managed by specific team, towards a more unified effort. (Gartner, 2024b)

Mobilization step's objective is to make sure that different teams of the organization can act and **transform findings into actionable security improvements** efficiently. Focus is gaining approvals and deploying mitigations to address identified vulnerabilities and exposures. This is achieved through **establishing clear communication protocols** to ensure all teams are aligned on the remediation requirements and processes. It also involves **documenting cross-team approval workflows to streamline decision-making** and the efficiency of the approval process across departments. (Gartner, 2022a)

Mobilization requires building strong relationships between the security team and other departments within an organization. Gartner states that identifying security issues often is not the main challenge; the challenges rather lie in agreeing on how to effectively resolve these issues and determining their priority with the departments that manage the affected assets. (Gartner, 2023c)

Gartner (2022b) also states that long term sustainable improvements made to the organizations cybersecurity should include at least, security, business, application architecture and Infrastructure & Operations (or I&O) team. (Gartner, 2022b)

Mobilization can start with creating a ticket in an **IT service management tool.** The remediation for the vulnerability or exposure might include **applying a technical control** or **an patch** to update the system and fix the vulnerability. (Gartner, 2022a)

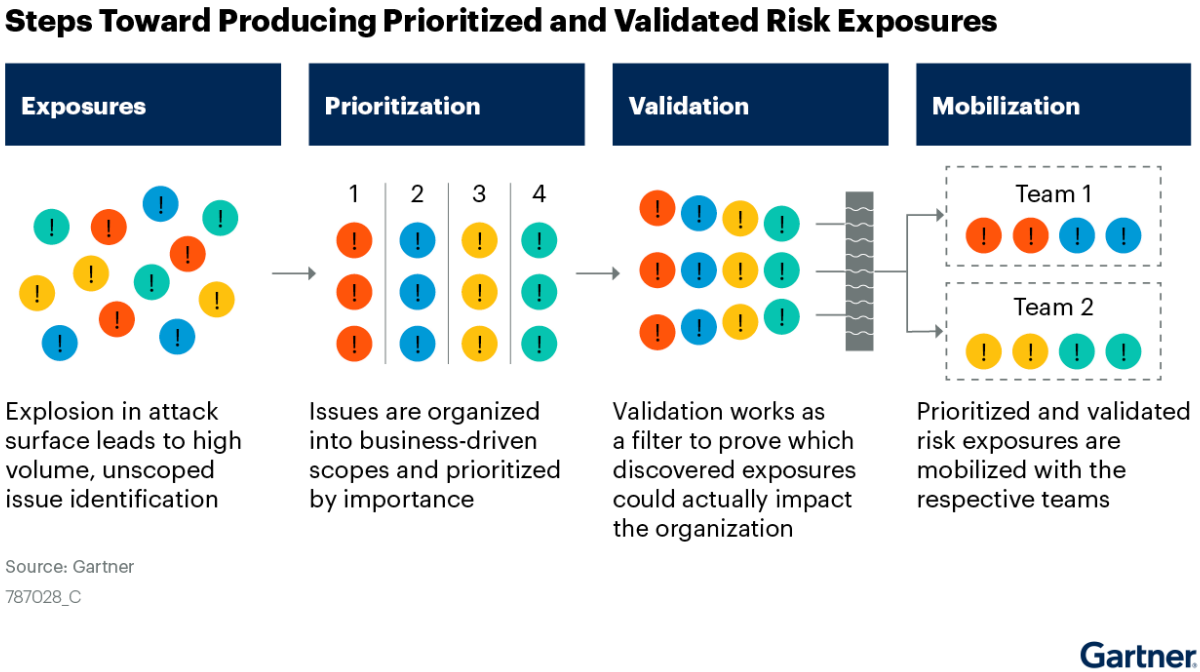

Figure 14. Steps toward producing priortized and validated risk exposures by Gartner (2023c)

The tools used in CTEM programs often automatically recommend these basic types of remediation based on the vulnerabilities they discover. This automation can help streamline the initial steps by suggesting straightforward, technical solutions that can be quickly implemented to reduce the immediate risk to the organization's IT environment. (Gartner, 2022a)

However, at the same time, Gartner advises to communicate to stakeholders that not all aspects of remediation can or should be automated. While **automated remediation**, which might include actions like patching vulnerabilities, **updating threat detection rules**, or **changing security configurations**, can efficiently address straightforward and minor issues, it has limitations. Mature organizations have found that relying solely on automation for resolving security issues is insufficient, as it often fails to address **more complex or nuanced vulnerabilities that require human judgment and intervention**. Gartner's publication concludes that *"There is no way for a tool or a security process to guess what will be acceptable for other teams."* (Gartner, 2022a)

Mobilization step comes to an end with the formal approval of required changes to address identified vulnerabilities or exposures, ensuring **alignment with organizational policies** and **securing**

stakeholder and business buy-in. Following approval, it is paramount to commit the necessary resources, including budget and personnel, to implement these changes effectively. Additionally, establishing an agreed-upon timeline with all stakeholders is essential for setting a clear schedule for remediation efforts, aiding in task prioritization and expectation management. (Gartner, 2022a)

Table 13. Mobilization capabilities

Mentioned capability	PPT category
transform findings into actionable security improvements	People
more complex or nuanced vulnerabilities that require human judgment and intervention	People
establishing clear communication protocols & documenting cross-team approval workflows to streamline decision-making	Process
alignment with organizational policies and securing stakeholder and business buy-in	Process
applying a technical control or an patch	Process
IT service management tool	Technology
automated remediation, which might include actions like patching vulnerabilities, updating threat detection rules, or changing security configurations	Technology

4.2 Summary of the CTEM

The summary figure ahead presents the recognized People, Process, and Technology capabilities across the 5 steps of the CTEM program.

Scoping	Discovery	Prioritization	Validation	Mobilization

People	Process	Technology
who are their (assets) owners and who are ultimately accountable for making risk decisions and changes regarding these assets	defines what areas, assets, or processes are most important to protect based on their value to the business	External attack surface -tool
taking the cyber adversaries mindset	consider how the risk would affect organizations crown jewels and how the business evaluates this risk	SaaS security posture –tool
identify other types of weaknesses, such as the presence of fake or unauthorized assets or poor results to phishing tests	identifying the assets within the scoped areas and assessing their risk profiles	Digital risk protection –tool
identify (organization's) high-value assets	finding vulnerabilities & identifying misconfigurations in assets and security controls	Dark and deep web sources
evaluation of the proposed treatments	newly identified assets and vulnerabilities should be noted and taken into account in subsequent CTEM cycles	Application, discovery, and host scanning
validate the response process to see that the organization is adequately prepared to handle real security incidents	assessing whether adequate security controls are already in place & evaluating the likelihood that these assets could be targeted and exploited by adversaries	Scanning of SaaS, code repositories, and third-party services
transform findings into actionable security improvements	usage of benchmarks to similar organizations and using historical data on past security breaches	threat intelligence data related to vulnerability or exposure
more complex or nuanced vulnerabilities that require human judgment and intervention	include the conclusion why something was deprioritized	Breach and Attack Simulation (BAS) systems and automated penetration testing tools
	potential attack the cyber adversaries could do against the detected vulnerability or exposure is assessed by the organization	IT service management tool
	assessment whether the exploitation of the exposure would be detected by the monitoring capabilities	automated remediation, which might include actions like patching vulnerabilities, updating threat detection rules, or changing security configurations
	Analyzing potential attack paths from initial vulnerabilities to critical business assets	
	Evaluating whether the organization's response and remediation processes are quick and effective enough to address vulnerabilities	
	red team exercises or contracting Penetration Testing as a Service (PTaaS) can be employed to simulate realistic attack scenarios	
	establishing clear communication protocols & documenting cross-team approval work-flows to streamline decision-making	
	alignment with organizational policies and securing stakeholder and business buy-in	
	applying a technical control or an patch	

Figure 15. Recognized PPT capabilities of CTEM

The purpose of the figure is to illustrate how each step, scoping, discovery, prioritization, validation, and mobilization, integrates these PPT capabilities to enhance the organization's cybersecurity posture. Figure presents how these different capabilities not only come together to complete a CTEM step, but also how they come together to complete the full CTEM program. The figure is used in the literature review part of this thesis to derive search terms for the literature review from the academic literature about SOCs existing capabilities to support CTEM program. This figure also answers this thesis' research question **RQ2**.

5 Literature review of SOCs applicability to CTEM programs

The literature review chapter presents the used data sources, search terms, selection of publications and evaluation process of the semi-structured literature review used in this thesis. Furthermore, this chapter will present the literature review's finding and the summary of the results. More detailed information of the literature review and its process is presented in the appendixes where creation of the search terms, selected publications and their evaluation and the actual literature review is presented.

5.1 Data sources

The selected data source where literature was searched for this thesis was decided to be Google Scholar. Google Scholar stands out as databases for conducting literature searches relevant to thesis due to their extensive and diverse repositories of scholarly articles. Google Scholar also conducts the searches to other relevant databases to the thesis, for example the IEEE Xplore.

When utilizing materials produced by various expert organizations and communities, it's advisable to research the nature of the institution involved. This is because think tanks, among others, also generate materials for their clients, which may lead to reports being somewhat biased or leaning towards a specific ideological or other direction. (Salminen, 2023). Gartner's sources and content was used on the chapter 4 regarding CTEM and not part of the literature review. Including Gartner as a source to the thesis acknowledges the crucial role that industry insights and trends play in both complementing academic and scientific research but also sometimes paving the way to academic research.

5.2 Breakdown of CTEM PPT capabilities into search terms

For the purposes of creating the search terms for literature review, the summary that was created in chapter 4 needs to be categorized and broken down for finding searchable entities. The breakdown done for the search terms is the following presented in the next figure, topline indicating to what domain is the recognized CTEM characteristic most associated with. The findings of chapter 3 were used to create the breakdown.

SOC management	Core Operations	Vulnerability Management	Threat Hunting	Red Teaming

People	Process	Technology
who are their (assets) owners and who are ultimately accountable for making risk decisions and changes regarding these assets	defines what areas, assets, or processes are most important to protect based on their value to the business	External attack surface -tool
taking the cyber adversaries mindset	consider how the risk would affect organizations crown jewels and how the business evaluates this risk	SaaS security posture –tool
identify other types of weaknesses, such as the presence of fake or unauthorized assets or poor results to phishing tests	identifying the assets within the scoped areas and assessing their risk profiles	Digital risk protection –tool
identify (organization's) high-value assets	finding vulnerabilities & identifying misconfigurations in assets and security controls	Dark and deep web sources
evaluation of the proposed treatments	newly identified assets and vulnerabilities should be noted and taken into account in subsequent CTEM cycles	Application, discovery, and host scanning
validate the response process to see that the organization is adequately prepared to handle real security incidents	assessing whether adequate security controls are already in place & evaluating the likelihood that these assets could be targeted and exploited by adversaries	Scanning of SaaS, code repositories, and third-party services
transform findings into actionable security improvements	usage of benchmarks to similar organizations and using historical data on past security breaches	threat intelligence data related to vulnerability or exposure
more complex or nuanced vulnerabilities that require human judgment and intervention	include the conclusion why something was deprioritized	Breach and Attack Simulation (BAS) systems and automated penetration testing tools
	potential attack the cyber adversaries could do against the detected vulnerability or exposure is assessed by the organization	IT service management tool
	assessment whether the exploitation of the exposure would be detected by the monitoring capabilities	automated remediation, which might include actions like patching vulnerabilities, updating threat detection rules, or changing security configurations
	Analyzing potential attack paths from initial vulnerabilities to critical business assets	
	Evaluating whether the organization's response and remediation processes are quick and effective enough to address vulnerabilities	
	red team exercises or contracting Penetration Testing as a Service (PTaaS) can be employed to simulate realistic attack scenarios	
	establishing clear communication protocols & documenting cross-team approval work-flows to streamline decision-making	
	alignment with organizational policies and securing stakeholder and business buy-in	
	applying a technical control or an patch	

Figure 16. Breakdown of CTEM PPT for literature review

As the reader can see, there are instances where certain CTEM characteristics could be relevant in multiple domains. The objective behind presenting the CTEM program's characteristics in relation

to the domains of SOC Management, Core Operations, Vulnerability Management, Threat Hunting and Red Teaming was not to provide an exhaustive categorization that considers every nuance and complexity of the recognized CTEM characteristic. Instead, the aim was to associate each characteristic of the CTEM program with the domain it most closely aligns with.

Categorizing the CTEM characteristics to these domains enables the more fluent creation of search terms for the literature review. The domains, that were already defined in this thesis, allow that associations between the CTEM characteristics themselves and existing practices can be highlighted and utilized in the research. By breaking down CTEM to these well-known domains, the author is allowed to create a smaller and more accurate set of search terms that will be used for searching the literature. The breakdown process to create the search terms is presented in Appendix 1.

5.3 Selection of publications

After the initial searches to the databases to retrieve the publications to be reviewed, the following steps were taken to qualify the publications for the thesis.

Following the breakdown in Figure 16. the following search terms were created to cover the different domains. The searches were done in Google Scholar between the 9th and the 10th of March 2024. When doing the searches, it was set that the publications should be released no later than 2019.

Table 14. Search terms used in Google Scholar during 9th and 10th of March 2024

ID	Search term	Total results
1	("Security Operations Center") AND ("risk assessment" OR "policy alignment")	706
2	("Security Operations Center") AND ("asset identification" OR "asset valuation")	56

3	("Security Operations Center") AND ("remediation process" OR "response process")	187
4	("Security Operations Center") AND ("ITSM" OR "digital risk protection" OR “SaaS security posture”)	72
5	("Security Operations Center") AND ("vulnerability identification" OR "vulnerability evaluation" OR "vulnerability remediation")	120
6	("Security Operations Center") AND ("external attack surface" OR "application scanning" OR "discovery scanning" OR "host scanning")	20
7	("Security Operations Center") AND ("weakness identification" OR "security improvements" OR "attack path analysis")	47
8	("Security Operations Center") AND ("detection capabilities")	221
9	("Security Operations Center") AND ("red teaming" OR "adversary mindset" OR "response validation" OR "Breach and Attack Simulation")	153

The process of evaluating the quality of the publications found in the search terms serves according to Okoli, 2015, two purposes. First prioritizing the publications based on their quality for the thesis and two to excluding publications that are not able to demonstrate the necessary methodological quality. The two purposes serve each other and thus the same review criteria can be used for both reviewing the quality of the publications and excluding the publications. Okoli points out that once the reviewer finds a publication that does not meet the required methodological standards these can be immediately excluded and need not be assessed for quality any further. (Okoli, 2015)

The initial 1510 searches from Google Scholar were reviewed by screening titles, abstract and the language of the publications. Publications that were obviously irrelevant to the study or which were in another language than English were discarded.

After these steps, the remaining 351 publications were screened in their abstracts to see if they would be suitable for the literature review, and they would be able to provide answers to the research questions. Also, the obtained publications, apart from Gartner, were available to Jyväskylä University of Applied Sciences students.

Regarding Gartner's publications, decision was made that publications that would be promoting any vendors or providers or highlighting their products or service offerings, would not be used. A total of 7 Gartner publications or sources were used for the thesis.

After these steps were done, 72 publications were selected to be assessed for the quality for the thesis. Questions in the following table were used to evaluate the quality of the gathered publications for this thesis. The publications were awarded points from 0-8 based on how many questions they gave a positive answer to. Decision was made to use only publications which would receive at least 7 points. None of the publications received the full 8 points. The reason was that no single publication was able to get a point from question 6.

Table 15. Questions presented to evaluate the quality of publications

Question 1	Is the publication based on scientific research or survey/interviews of IT/cyber professionals?
Question 2	Does the publication have a clear goal?
Question 3	Are the conclusions presented clearly?
Question 4	Is the term 'SOC' defined and it contains relevant information for this thesis?
Question 5	Is the People, Processes and Technologies (PPT) framework or similar referred in the publication?
Question 6	Does the publication mention Continuous Threat Exposure Management or CTEM?
Question 7	Does the publication discuss how SOC should be integrated to the organization's other processes and teams?
Question 8	Are examples of SOC PPT capabilities and teams' integration to the organization given which are relevant to the thesis?

In the end, for the literature review, 13 publications were used. The publications and evaluations were tracked on a table which allowed fast and clear review of the quality of the selected publications and provided a method for scoring and excluding the publications. The table can be found in Appendix 2. Selected publications and scoring. The whole data collection phase is illustrated in the PRISMA figure below.

According to Page et al., the Preferred Reporting Items for Systematic reviews and Meta-Analyses, or PRISMA, was created to assist systematic reviewers in clearly explaining the purpose of the review, the methods used by the authors, and their findings. (Page et al., 2021)

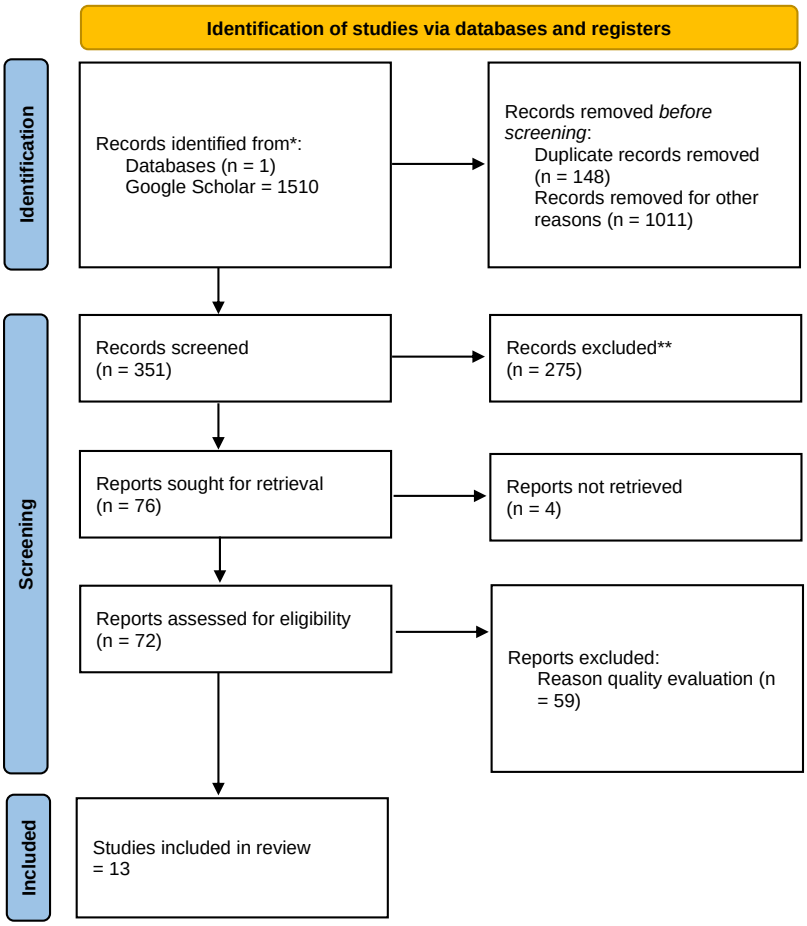

Figure 17. PRISMA diagram for this thesis, adapted from Page et al. (2021)

In the following chapters 5.4 to 5.6 we will go through how the literature review managed to respond to the different People, Process and Technology capabilities of CTEM that were recognized in chapter 4. The IDs given to CTEM capabilities (Pe1, Pr1, T1 etc.) will be used in the subchapters

5.4 to 5.6. and again, in the summary chapter 5.7. The full description of the individual literature contents and results can be found in Appendix 3. Literature review results.

5.4 People applicability

From the People applicability perspective, the literature could provide answers to 6 out of 8 CTEM capabilities. The remaining two were partially answered.

Table 16. People applicability

ID	CTEM capability	SOC literature, ID visible in Appendix 2 & 3
Pe1	who are their (assets) owners and who are ultimately accountable for making risk decisions and changes regarding these assets	Asset owners and people that can make risk decisions are recognized by SOC during the onboarding of the service or when changes to the monitored assets are happening. ***Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.***
Pe2	taking the cyber adversaries mindset	During red teaming and threat hunting, which can be both be offered by SOCs, the idea is to take the adversary mindset. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pe3	identify other types of weaknesses, such as the presence of fake or unauthorized assets or poor results to phishing tests	Both red teaming and threat hunting can take a look at potential organizational weaknesses in new angles. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pe4	identify (organization's) high-value assets	Identification of these is usually part of the onboarding. ***Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.***
Pe5	evaluation of the proposed treatments	Not addressed in the literature review. Validation of threat detection capabilities and detection use cases were mentioned. One publication described the SOC roles for Security Control Assessor and System Testing and Evaluation Specialist. Role descriptions given utilizing the European Union Agency for Cybersecurity (ENISA) European Cybersecurity Skills Framework (ECSF) tool. ***Demonstrated in Erdıvan, C. (2024) ID 21.***

Pe6	validate the response process to see that the organization is adequately prepared to handle real security incidents	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pe7	transform findings into actionable security improvements	Security risk assessment should prioritize what services SOC will offer. The risk assessment should identify what security controls are in place and where gaps currently are. Also, threat hunting, red teaming and vulnerability management should also provide improvements based on their findings. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15; Rodman, C. et al. (2024) ID 56.***
Pe8	more complex or nuanced vulnerabilities that require human judgment and intervention	Not addressed in the literature review. Many of the publications highlighted the importance of teamwork. One publication mentions that be able to detect unknown attacks the use of non-security people, like engineers, will become more important in the future. ***Demonstrated in Vielberth, M. et al. (2020) ID 70.***

5.5 Process applicability

From the Process applicability perspective, the literature could provide answers to 13 out of 16 CTEM capabilities. One capability was partially answered, while for there was no answer retrieved from literature.

Table 17. Process applicability

ID	CTEM capability	SOC literature, ID visible in Appendix 2 & 3
Pr1	defines what areas, assets, or processes are most important to protect based on their value to the business	These are usually done during onboarding, but as it was also mentioned in the document 46, there is a necessity that this continuously assed when changes to the environment happen.

		Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.
Pr2	consider how the risk would affect organizations crown jewels and how the business evaluates this risk	Usually this is done as part of the onboarding activities but should be taken into account when changes take place. ***Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.***
Pr3	identifying the assets within the scoped areas and assessing their risk profiles	These are usually done during onboarding, but as it was also mentioned in the document 46, there is a necessity that this continuously assessed when changes to the environment happen. Also, utilization of threat modeling to define scope, determine log sources, select appropriate tools and technologies to your SOC. In case of a large organizational environment, priority for SOC building should be given to high-risk businesses. ***Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.***
Pr4	finding vulnerabilities & identifying misconfigurations in assets and security controls	Vulnerability scanning can be one of the services that SOC offers. ***Demonstrated in Rehman, R. (2019) ID 54.***
Pr5	newly identified assets and vulnerabilities should be noted and taken into account in subsequent CTEM cycles	Not addressed in the literature review. However, usually this is considered standard practice in vulnerability management.
Pr6	assessing whether adequate security controls are already in place & evaluating the likelihood that these assets could be targeted and exploited by adversaries	Security risk assessment should identify what security controls are in place and where gaps currently are. Also red teaming and threat hunting should aim to provide input on the likelihood and validity of certain attack vectors. ***Demonstrated in AlAhmadi, B. A. (2019) ID 4; Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15; Rodman, C. et al. (2024) ID 56.***

Pr7	usage of benchmarks to similar organizations and using historical data on past security breaches	Could be done as part of the strategic level cyber threat intelligence efforts done by SOC. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Rehman, R. (2019) ID 54.***
Pr8	include the conclusion why something was deprioritized	Not addressed in the literature review.
Pr9	potential attack the cyber adversaries could do against the detected vulnerability or exposure is assessed by the organization	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pr10	assessment whether the exploitation of the exposure would be detected by the monitoring capabilities	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pr11	Analyzing potential attack paths from initial vulnerabilities to critical business assets	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10, Crichlow, M. C. (2020) ID 15.***
Pr12	Evaluating whether the organization's response and remediation processes are quick and effective enough to address vulnerabilities	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pr13	red team exercises or contracting Penetration Testing as a Service (PTaaS) can be employed to simulate realistic attack scenarios	This activity can be part of red teaming and threat hunting. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Crichlow, M. C. (2020) ID 15.***
Pr14	establishing clear communication protocols & documenting cross-team approval work-flows to streamline decision-making	Among the essential technologies is mentioned ticketing system and workflow tools. One publication stated that in the future, collaboration needs between SOC and departments like IT and compliance will increase. One publication also mentioned that SOC functions as communication bridge between IT departments and other parts of the organization and promotes collaboration. ***Demonstrated in Bhardwaj, A. (2021) ID 9;***

		Majid, M. A., & Ariffin, K. A. Z. (2021) ID 42; Mughal, A. A. (2022) ID 43; Rodman, C. et al. (2024) ID 56.
Pr15	alignment with organizational policies and securing stakeholder and business buy-in	Alignment efforts are usually done during onboarding. Entities such as SOC Governance Board with relevant stakeholders and creation of policies for SOC and teams that SOC needs to work with have been presented to address these. Examples of policies can be log collection and incident identification and escalation policies. ***Demonstrated in Onwubiko (2021) ID 46; Rehman, R. (2019) ID 54.***
Pr16	applying a technical control or an patch	Not addressed in the literature review. One publication states that the organizational program for this can be run by SOC or by a separate team. Regarding patch management, point is made that SOC, for its own infrastructures patching, should follow the organizations patch management process. ***Demonstrated in Rodman, C. et al. (2024) ID 56.***

5.6 Technology applicability

From the Technology applicability perspective, the literature could provide answers to 5 out of 10 CTEM capabilities. The remaining 5 were unanswered by the selected literature.

Table 18. Technology applicability

ID	CTEM capability	SOC literature, ID visible in Appendix 2 & 3
T1	External attack surface -tool	Not addressed in the literature review. Literature mentioning this was not retrievable during the data collection phase.
T2	SaaS security posture –tool	Not addressed in the literature review.
T3	Digital risk protection –tool	Not addressed in the literature review.

T4	Dark and deep web sources	Part of the cyber threat intelligence efforts done by SOC. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Rehman, R. (2019) ID 54.***
T5	Application, discovery, and host scanning	Part of vulnerability scanning or vulnerability management. ***Demonstrated in AlAhmadi, B. A. (2019) ID 4; Dun, Y. T. et al. (2021) ID 20; Erdıvan, C. (2024) ID 21; Majid, M. A., & Ariffin, K. A. Z. (2021) ID 42.***
T6	Scanning of SaaS, code repositories, and third-party services	Not addressed in the literature review.
T7	threat intelligence data related to vulnerability or exposure	Part of the cyber threat intelligence efforts done by SOC. ***Demonstrated in Bolla, A., & Talentino, F. (2022) ID 10; Rehman, R. (2019) ID 54.***
T8	Breach and Attack Simulation (BAS) systems and automated penetration testing tools	Not addressed in the literature review.
T9	IT service management tool	Among the essential technologies is mentioned ticketing system and workflow tools. ***Demonstrated in Rodman, C. et al. (2024) ID 56.***
T10	automated remediation, which might include actions like patching vulnerabilities, updating threat detection rules, or changing security configurations	Many publications highlighted that automation is something that is needed more in the future, but the underlying message was that this is taking place. One publication predicted that automation and AI will handle increasingly larger portion of the incidents in the future. Another publication presented that onboarding's future state in cloud environment's is done via automation and that minimal hands-on effort is required. One publication argues that being able to automate requires working with teams from different domains of the organization. Doing automation might require a periodic meeting where different work efforts are examined to recognize possibilities for automation. ***Demonstrated in Mughal, A. A. (2022) ID 43; Onwubiko, C. (2021) ID 46; Revaclier, A. R. (2021) ID 55.***

5.7 Summary of the literature review's results

As we compile the literature review's results together, we can see that there were 24 capabilities of CTEM that the literature review was able to answer out of the total 34 capabilities. This provides us the answer for the research question **RQ1**.

SOC management	Core Operations	Vulnerability Management	Threat Hunting	Red Teaming

People	Process	Technology
Pe1 – Demonstrated capability	Pr1 – Demonstrated capability	**T1 – Not addressed in literature review**
Pe2 – Demonstrated capability	Pr2 – Demonstrated capability	**T2 – Not addressed in literature review**
Pe3 – Demonstrated capability	Pr3 – Demonstrated capability	**T3 – Not addressed in literature review**
Pe4 – Demonstrated capability	Pr4 – Demonstrated capability	T4 – Demonstrated capability
Pe5 – Not addressed in literature review	**Pr5 – Not addressed in literature review**	T5 – Demonstrated capability
Pe6 – Demonstrated capability	Pr6 – Demonstrated capability	**T6 – Not addressed in literature review**
Pe7 – Demonstrated capability	Pr7 – Demonstrated capability	T7 – Demonstrated capability
Pe8 – Not addressed in literature review	**Pr8 – Not addressed in literature review**	**T8 – Not addressed in literature review**
	Pr9 – Demonstrated capability	T9 – Demonstrated capability
	Pr10 – Demonstrated capability	T10 – Demonstrated capability
	Pr11 – Demonstrated capability	
	Pr12 – Demonstrated capability	
	Pr13 – Demonstrated capability	
	Pr14 – Demonstrated capability	
	Pr15 – Demonstrated capability	
	Pr16 – Not addressed in literature review	

Figure 18. Summary of literature reviews results

The largest amount of non-addressed capabilities was in the Technology domain, with 5 non-addressed capabilities. All the non-addressed capabilities in People and Process, and two in the technology domain were categorized to the Vulnerability Management domain. These findings provide us the answer to research question **RQ3**.

6 Conclusion

The thesis successfully managed to answer the research questions it set out to answer. What became more evident to the author as part of the research process was that the SOC as an organization lacks the overarching definitive decision of its capabilities and contents. Author feels that Knerler et al. defined it best by stating that *"SOC is defined primarily by what it does: cyber defence"*. What was new information to the author was the definition of CTEM and how much more

it is a type of security framework rather than strict standard. Author finds many similarities with CTEM approach to the better known Zero Trust security framework, where actually what PPT characteristics your organization has and what its business objectives are should determine what type of a Zero Trust model you end up building to your organization. Therefore, there is room for argumentation about this thesis' findings.

In terms of the SOCs existing capabilities and gaps to enable or support CTEM program one can always state that 'it will depend on the SOC', which the author finds an accurate statement. As it was defined already in chapter 3.2 by Knerler et al. the SOCs core activities typically are alert monitoring and incident triage. However, some of the SOCs might have other capabilities such as vulnerability scanning, penetration testing or threat hunting. If these other capabilities are offered by other team in the organization, an external partner or not at all, these are of course a capability that would be lacking from the SOC. Then it would be the organization's decision to determine if this would be a future SOC capability that the organization would need to invest in, or if the alternative ways to produce this capability are now sufficient.

In terms of the overall CTEM capabilities that the research found, the author can conclude that there can be great possibilities for the SOC enable or support the organization's CTEM program. SOC's usually are aware of the organization's assets, they have well-defined and traceable workflows, and they are accustomed to communicating and having discussions with other teams in the organization in order to understand the business objectives for security monitoring and building monitoring capabilities to new assets and places. Evaluation of their own capabilities in terms of detection and response capabilities and taking the adversary mindset are also something that even somewhat mature SOCs should be able to do.

Also, the author finds that the findings about the potential gaps about SOC's capabilities to support CTEM in terms of vulnerability management is accurate. Vulnerability management is something that SOCs can do and are doing when it is about detecting and reporting vulnerabilities, but when it comes to assessing the criticality of the found vulnerabilities while taking into account where the vulnerable asset is located, what is it used to and if the vulnerable component is even in use, is something that the team responsible for the vulnerable asset is only able to determine.

As the conclusion, author finds that the SOC can be the enablers and supporters of the CTEM program, but the characteristics of this enablement or support will be always determined by the capabilities of the SOC, the capabilities of the organization, and how they decide they will conduct their cooperation. Also, it is good to note that the capabilities of the SOC could very well be in some organization's CTEM programs scope in the future.

6.1 Evaluation of reliability and ethicality of results

The reliability of the research was created and maintained by following the set research methodology during the thesis process and utilizing previous academic research and professional literature about the studied subjects. As it was stated in the Background and motivation -chapter for this thesis, this research was conducted out of personal and professional interest of the author. The thesis leveraged author's practical experience in sales and service management of SOC services. This research was conducted under the sole direction of the author and no other entities were affiliated with the research. Author thus declares that he has no conflict of interest.

The literature review process was conducted with transparency by presenting the search term creation, the found literature, the evaluation process of the literature and the literature review findings. Detailed information for all of these were provided in the attached appendixes. The evaluation process enforced the author to choose both recent and high quality academic and professional literature for the purposes of the research.

Regarding the chapters about CTEM, only Gartner content which did not feature or mention any service providers or organizations were used. The used content was Gartner's subscribed material for their customers and can be thus characterized having more content and providing more in-depth information on the subject matter than material that is made publicly available. Gartner was contacted by the author before any content was created for this thesis using Gartner's subscribed material. The CTEM content was created by the author when the consent was obtained, and Gartner reviewed the created content before it was published. Gartner has thus ensured that its content has been portrayed correctly by the author.

To address the ethical considerations, the author followed and abided the JAMK's ethical and thesis guidelines. The references and the collected data were presented in a transparent way so that

the readers can come to the same results as the author has. The readers of the thesis can go through the chapters and trace how the author has created the summaries and figures made to chapters 3, 4 and 5.

6.2 Suggestions for further research

As its current academic literature showcases, the Continuous Threat Exposure Management is still an unexplored topic. In case in the future more and more organizations will be initiating their CTEM programs hopefully this will spring more all types of academic literature regarding CTEM and its characteristics. For the author, interesting research would be examples where to real-life or mockup organizations a CTEM program flowchart would be created. This flowchart would visualize the interfaces in that organization's CTEM program and would showcase the teams and their responsibilities for CTEM. This would also allow examining where would be the responsibilities and interfaces for a SOC to enable or support a CTEM program.

References

5G/SOC: SOC Generations. (2013). Hewlett-Packard Development Company. http://www.cnmeonline.com/myresources/hpe/docs/HP_ArcSight_WhitePapers_5GSOC_SOC_Generations.PDF

Agarwal, A., Walia, H., & Gupta, H. (2021). Cyber Security Model for Threat Hunting. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–8. https://doi.org/10.1109/ICRITO51393.2021.9596199

Arfeen, A., Ahmed, S., Khan, M. A., & Jafri, S. F. A. (2021). Endpoint Detection & Response: A Malware Identification Solution. *2021 International Conference on Cyber Warfare and Security (ICCWS)*, 1–8. https://doi.org/10.1109/ICCWS53234.2021.9703010

Baek, S., & Kim, Y.-G. (2019). Efficient Vulnerability Management Process in the Military. *2019 International Conference on Platform Technology and Service (PlatCon)*, 1–5. https://doi.org/10.1109/PlatCon.2019.8669420

Bautista, W. (2018). *Practical cyber intelligence: How action-based intelligence can be an effective response to incidents* (First published: March 2018). Packt Publishing.

Chuvakin, D. A. (2016). *The Complete Guide to Log and Event Management*. https://www.netiq.com/en-gb/docrep/documents/m47h82fbmy/the_complete_guide_to_log_and_event_management_wp_ee.pdf

Dandurand, L., & Serrano, O. S. (2013). *Towards Improved Cyber Security Information Sharing*. https://ccdcoe.org/uploads/2018/10/25_d3r1s5_dandurand.pdf

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity, attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing.

Firstbrook, P., Ouellet, E., & Mcshane, I. (2017). *Redefining Endpoint Protection for 2017 and 2018*. https://www.gartner.com/en/documents/3803522

Gartner. (2023c). *2024 Strategic Roadmap for Managing Threat Exposure*. Shoard, P. Published 8 November 2023.

Gartner. (2024a). *Do you have a CTEM (continuous threat exposure management) program? | Gartner Peer Community*. https://www.gartner.com/peer-community/poll/have-ctem-continuous-threat-exposure-management-program

Gartner. (2022a). *Implement a Continuous Threat Exposure Management (CTEM) Program*. D'Hoinne, J., Shoard, P., Schneider, M. Published 21 July 2022. This Gartner report is archived and is included for historical context only. GARTNER is a trademark of Gartner Inc. and/or its affiliates.

Gartner. (2022b). *Predicts 2023: Enterprises Must Expand From Threat to Exposure Management*. D'Hoinne, J., Shoard, P., Schneider, M. Watts, J. Published 1 December 2022. This Gartner report is archived and is included for historical context only.

Gartner. (2023a). *Top Strategic Technology Trends for 2024*. Willemsen, B., Olliffe, G., Chandrasekaran, A. Published 16 October 2023.

Gartner. (2023b). *Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management*. D'Hoinne, J., Shoard, P. Published 16 October 2023.

Gartner. (2024b). *Top Strategic Technology Trends in China for 2024: Continuous Threat Exposure Management*. Zhao, A. Published 5 February 2024.

GovCERT-HK. (2023). Security Incident Handling for Companies. *GovCERT-HK*. https://www.infosec.gov.hk/en/best-practices/business/security-incident-handling-for-companies

Hirsjärvi, S., Remes, P., Sajavaara, P., & Sinivuori, E. (2010). *Tutki ja kirjoita* (15.-16. p). Tammi.

Hlupic, T., Orescanin, D., Ruzak, D., & Baranovic, M. (2022). An Overview of Current Data Lake Architecture Models. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1082–1087. https://doi.org/10.23919/MIPRO55190.2022.9803717

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G.-J. (2019). Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 1955–1970. https://doi.org/10.1145/3319535.3354239

Mutemwa, M., Mtsweni, J., & Zimba, L. (2018). Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–6. https://doi.org/10.1109/ICONIC.2018.8601251

Neil, I. (2018). *CompTIA Security+ Certification Guide*. Packt Publishing.

Onwubiko, C. (2021). Rethinking Security Operations Centre Onboarding. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–9. https://doi.org/10.1109/CyberSA52016.2021.9478245

Orsos, M., Kecskes, M., Kail, E., & Banati, A. (2022). Log collection and SIEM for 5G SOC. *2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 000147–000152. https://doi.org/10.1109/SAMI54271.2022.9780759

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Podzins, O., & Romanovs, A. (2019). Why SIEM is Irreplaceable in a Secure IT Environment? *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, 1–5. https://doi.org/10.1109/eStream.2019.8732173

Prodan, M., Prodan, A., & Purcarea, A. A. (2015). Three New Dimensions to People, Process, Technology Improvement Model. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies* (Vol. 353, pp. 481–490). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_47

Salminen, A. (2023). *Mikä kirjallisuuskatsaus? : Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. https://osuva.uwasa.fi/bitstream/handle/10024/15470/978-952-395-081-8%20%28PDF%29.pdf?sequence=2&isAllowed=y

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sridharan, A., & Kanchana, V. (2022). SIEM integration with SOAR. *2022 International Conference on Futuristic Technologies (INCOFT)*, 1–6. https://doi.org/10.1109/INCOFT55651.2022.10094537

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

Villalon-Huerta, A., Gisbert, H. M., & Ripoll-Ripoll, I. (2022). SOC Critical Path: A Defensive Kill Chain Model. *IEEE Access*, *10*, 13570–13581. https://doi.org/10.1109/ACCESS.2022.3145029

What is Gartner? – TechTarget Definition. (n.d.). WhatIs. Retrieved February 15, 2024, from https://www.techtarget.com/whatis/definition/Gartner

Zagan, E., & Danubianu, M. (2021). Cloud DATA LAKE: The new trend of data storage. *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 1–4. https://doi.org/10.1109/HORA52670.2021.9461293

Appendices

Appendix 1. Creation of search terms for literature review

The recognized People, Process and Technology capabilities of CTEM done in chapter 4 were divided into five different operative domains that were all presented in chapter 3. The objective was to find the closest operative domain to the described PPT capability. In close cases where the PPT capability could be part of two or several domains, a decision was made to include it in a single domain.

After this, the operative domains, or colors, were investigated individually to review their PPT capabilities and to create search terms from them. The idea of the search terms was to be as encompassing as possible without creating too many search terms. The idea was to both limit the amount of search terms and to come up with more high-quality literature in the data collection.

Search terms created and used for the data collection:

Domain: SOC management

1. ("Security Operations Center") AND ("risk assessment" OR "policy alignment")
2. ("Security Operations Center") AND ("asset identification" OR "asset valuation")

Domain: Core Operations

3. ("Security Operations Center") AND ("remediation process" OR "response process")
4. ("Security Operations Center") AND ("ITSM" OR "digital risk protection" OR “SaaS security posture”)

Domain: Vulnerability management

5. ("Security Operations Center") AND ("vulnerability identification" OR "vulnerability evaluation" OR "vulnerability remediation")
6. ("Security Operations Center") AND ("external attack surface" OR "application scanning" OR "discovery scanning" OR "host scanning")

Domain: Threat hunting

7. ("Security Operations Center") AND ("weakness identification" OR "security improvements" OR "attack path analysis")
8. ("Security Operations Center") AND ("detection capabilities")

Domain: Red teaming

9. ("Security Operations Center") AND ("red teaming" OR "adversary mindset" OR "response validation" OR "Breach and Attack Simulation")

Appendix 2. Selected publications and scoring

ID	Publication name	Year published
1	Integrated threat intelligence platform for security operations in organizations	2024
2	Attack Techniques and Threat Identification for Vulnerabilities	2022
3	Incident Handling and Response Process in Security Operations	2023
4	Malware detection in security operation centres	2019
5	A QUALITATIVE STUDY ON SECURITY OPERATIONS CENTERS IN SAUDI ARABIA: CHALLENGES AND RESEARCH DIRECTIONS	2020
6	The Role of Artificial Intelligence and Machine Learning in Shaping the Future of Cybersecurity: Trends, Applications, and Ethical Considerations	2023
7	SaaS Investigation Tool	2022
8	An Automated Post-Exploitation Model for Offensive Cyberspace Operations	2022
9	Impacts of IoT on Industry 4.0: Opportunities, Challenges, and Prospects	2021
10	Threat Hunting driven by Cyber Threat Intelligence	2022
11	Securing a Remote Workforce	2021
12	Challenges around Information Security Management in the Public Cloud	2021
13	Technical Guide for Implementing Cybersecurity Continuous Monitoring in the Nuclear Industry	2021
14	Cyber Threat Intelligence: Current Trends and Future Perspectives	2023
15	A study on Blue Team's OPSEC failures	2020
16	Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey	2019
17	A SANS 2021 Survey: Security Operations Center (SOC)	2021
18	Security Operations Center: A Framework for Automated Triage, Containment and Escalation	2020
19	A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making	2024
20	Grasp on next generation security operation centre (NGSOC): Comparative study	2021
21	Process, Technology and Human Aspects of a Security Operations Center	2024
22	Continuous improvement on maturity and capability of security operation centers	2019
23	Review of Industry 4.0 Challenges	2021
24	Breach and Attack Simulator	2022
25	Measuring the Technical Performance of a Security Operations Center	2022
26	Technical performance metrics of a security operations center	2023
27	Extending Detection and Response: How MXDR Evolves Cybersecurity	2023
28	Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges	2023
29	Perspectives on risk prioritization of data center vulnerabilities using rank aggregation and multi-objective optimization (arXiv:2202	2022
30	Towards More Insight into Cyber Incident Response Decision Making and its Implications for Cyber Crisis Management	2022
31	Myths and Misconceptions about Attackers and Attacks	2021
32	The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system	2019
33	Understanding Threat Hunting Personas	2023
34	From SOC to VSOC: Transferring Key Requirements for Efficient Vehicle Security Operations	2023
35	Measuring and Improving Cyber Defense Using the MITRE ATT&CK Framework	2023
36	Intrusion Detection & Incident Response for Information Security: Technologies and Challenges	2022
37	Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response	2023
38	An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors	2021
39	Automation in cyber security	2021
40	AI/ML in Security Orchestration, Automation and Response: Future Research Directions	2021
41	Success Factors for Cyber Security Operation Center (SOC) Establishment	2019
42	Model for successful development and implementation of Cyber Security Operations Centre (SOC)	2021
43	Building and Securing the Modern Security Operations Center (SOC)	2022
44	Detecting cyber attacks in time: Combining attack simulation with detection logic	2021
45	A Survey on Threat Hunting in Enterprise Networks	2023
46	Rethinking Security Operations Centre Onboarding	2021
47	The Next Gen Security Operation Center	2021
48	Why SIEM is Irreplaceable in a Secure IT Environment?	2019
49	Simplification of application operations using cloud and DevOps	2019
50	Identifying and estimating cybersecurity risk for enterprise risk management	2021
51	Improving Computer Security Incident Response Team: Establishment & Operation	2022
52	Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center	2021
53	Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field	2023
54	Cybersecurity Arm Wrestling	2019
55	SOC-AM: An Accessible Maturity Model for Security Operation Centers	2021
56	SOC Service Areas: Identification, Prioritization, and Implementation	2024
57	An OSINT Approach to Automated Asset Discovery and Monitoring	2019
58	Red Teaming: Regulatory and non-regulatory frameworks used in adversarial simulations	2021
59	Threat Management Based on Information About Vulnerabilities	2020
60	Automated Identification of Cyber Threat Scenarios	2022
61	Vulnerability Selection for Remediation: An Empirical Analysis	2022
62	Integrated Network and Security Operation Center: A Systematic Analysis	2022
63	Effective Security Monitoring Using Efficient SIEM Architecture	2023
64	Automating Correlation Between Attacks and Detection in Purple Team Exercises	2023
65	Modeling a Security Operations Center	2022
66	Cyber security services reporting framework	2021
67	Why Cyber Threat Modeling Needs Human Factors Expansion: A Position Paper	2023
68	Developing decision support for cybersecurity threat and incident managers	2022
69	Attack Surface Management: Principles for simplifying the complexity of OT security	2023
70	Security Operations Center: A Systematic Study and Open Challenges	2022
71	SOC Critical Path: A Defensive Kill Chain Model	2022
72	An Attack Simulation Methodology for Empirical SOC Performance Evaluation	2019

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Resul
1	1	1	1	1	0	0	0	0	4
2	1	1	1	0	0	0	0	0	3
3	1	1	1	1	0	0	1	0	5
4	1	1	1	1	1	0	1	1	7
5	1	1	1	1	1	0	0	0	5
6	1	1	1	0	0	0	0	0	3
7	1	1	1	1	1	0	0	0	5
8	1	1	1	1	0	0	0	0	4
9	1	1	1	1	1	0	1	1	7
10	1	1	1	1	1	0	1	1	7
11	1	1	1	0	0	0	0	0	3
12	1	1	1	0	0	0	0	0	3
13	1	1	1	0	0	0	0	0	3
14	1	1	1	0	1	0	0	0	4
15	1	1	1	1	1	0	1	1	7
16	1	1	1	1	1	0	1	0	6
17	1	1	1	1	0	0	1	1	6
18	1	1	1	1	1	0	1	0	6
19	1	1	1	0	1	0	0	0	4
20	1	1	1	1	1	0	1	1	7
21	1	1	1	1	1	0	1	1	7
22	1	1	1	1	1	0	1	0	6
23	1	1	1	1	0	0	1	1	6
24	1	1	1	1	0	0	1	1	6
25	1	1	1	1	1	0	1	0	6
26	1	1	1	1	1	0	1	0	6
27	1	1	1	1	0	0	1	1	6
28	1	1	1	1	0	0	0	0	4
29	1	1	1	0	0	0	0	0	3
30	1	1	1	1	0	0	0	0	4
31	1	1	1	0	0	0	0	0	3
32	1	1	1	0	0	0	0	0	3
33	1	1	1	0	0	0	0	0	3
34	1	1	1	1	1	0	1	0	6
35	1	1	1	0	0	0	0	1	4
36	1	1	1	1	0	0	1	1	6
37	1	1	1	0	0	0	0	0	3
38	1	1	1	1	0	0	1	0	5
39	1	1	1	1	0	0	0	0	4
40	1	1	1	1	0	0	1	1	6
41	1	1	1	1	1	0	1	0	6
42	1	1	1	1	1	0	1	1	7
43	1	1	1	1	1	0	1	1	7
44	1	1	1	1	0	0	1	1	6
45	1	1	1	1	0	0	1	1	6
46	1	1	1	1	1	0	1	1	7
47	1	1	1	1	1	0	1	0	6
48	1	1	1	1	1	0	0	0	5
49	1	1	1	0	0	0	0	0	3
50	1	1	1	0	0	0	0	0	3
51	1	1	1	0	0	0	0	0	3
52	1	1	1	1	1	0	0	0	5
53	1	1	1	0	0	0	0	0	3
54	1	1	1	1	1	0	1	1	7
55	1	1	1	1	1	0	1	1	7
56	1	1	1	1	1	0	1	1	7
57	1	1	1	1	0	0	1	1	6
58	1	1	1	1	1	0	0	0	5
59	1	1	1	1	1	0	1	0	6
60	1	1	1	1	1	0	1	0	6
61	1	1	1	1	0	0	1	1	6
62	1	1	1	1	1	0	1	0	6
63	1	1	1	0	0	0	0	0	3
64	1	1	1	0	0	0	0	0	3
65	1	1	1	1	0	0	0	0	4
66	1	1	1	0	0	0	0	0	3
67	1	1	1	1	0	0	1	1	6
68	1	1	1	1	0	0	1	1	6
69	1	1	1	0	0	0	0	0	3
70	1	1	1	1	1	0	1	1	7
71	1	1	1	1	1	0	1	0	6
72	1	1	1	1	1	0	1	0	6

Appendix 3. Literature review results

ID	Publication	SOC domain relates most	How the publication relates to CTEM PPT properties
4	Malware detection in security operation centres. AlAhmadi, B. A. (2019)	Vulnerability Management	People: mentions that SOC staffed with security analysts, engineers, incident responders, hunters, contractors, as well as managers. Process: mentions various SOC workflows that personnel follow, risk assessments for each customers and assets are different. Technology: mentions various technological solutions used by SOCs such as Asset Discovery, Vulnerability Assessment, Behavioural Monitoring, Signature-based Intrusion Detection Systems, and SIEMs.
9	Impacts of IoT on Industry 4.0: Opportunities, Challenges, and Prospects. Bhardwaj, A. (2021)	Core Operations	People: SOC functions as communication bridge between IT departments and other parts of the organization and promotes collaboration. Process: SOC facilitates coordination and controls over IT processes and regulations Technology: SOC offers real-time threat awareness, and generates comprehensive reports about network, system, and application security status
10	Threat Hunting driven by Cyber Threat Intelligence. Bolla, A., & Talentino, F. (2022)	Threat Hunting	People: SOC employs a team, led by a SOC manager and including SOC analyst and threat hunters Process: Cyber threat intelligence collection and use process in SOC. Cyber Threat Hunting for proactively searching for advanced threats and malicious behaviours inside of systems, organizations, endpoints and networks. Technology: Emphasizing the use of Predictive Analysis in the future. This leverages Artificial Intelligence and Machine Learning capabilities, behavioural analysis and, in general, implementing multi-techniques prevention systems.

ID	Publication	SOC domain relates most	How the publication relates to CTEM PPT properties
15	A study on Blue Team's OPSEC failures. Crichlow, M. C. (2020)	Red Teaming	People: Red teaming as a core idea is to look at a problem form an adversary or competitor perspective. Process: Evaluating Blue team responses. Wargaming as a tool for observing the attacker and defender interaction. Technology: Red team technology to detect Blue team efforts.
20	Grasp on next generation security operation centre (NGSOC): Comparative study. Dun, Y. T. et al. (2021)	Core Operations	People: The protection task of the SOC calls for stakeholders to be informed and apply adequate protections to protect the data and critical framework at the risk of cyber security occurrences. Process: The functionality of a SOC—its ability to effectively perform its intended roles—derives strength from how well it is defined and integrated into the organization. Technology: Mentions tools used by SOCs including: Continuous Vulnerability Assessment, Vulnerability Management, Asset Management, eDiscovery
21	Process, Technology and Human Aspects of a Security Operations Center. Erdıvan, C. (2024)	Core Operations	People: Describes possible SOC roles for example, Security Control Assessor and System Testing and Evaluation Specialist. Role descriptions given utilizing ENISA European Cybersecurity Skills Framework (ECSF) tool. Process: Describes the processes within a SOC, including log management, incident response, and vulnerability management, essential for identifying, prioritizing, and addressing threats. Technology: Discusses the deployment and utilization of various technologies such as SIEM, firewalls, IDS/IPS, and more.

ID	Publication	SOC domain relates most	How the publication relates to CTEM PPT properties
42	Model for successful development and implementation of Cyber Security Operations Centre (SOC). Majid, M. A., & Ariffin, K. A. Z. (2021)	SOC Management	People: Emphasizes the importance of communication as a tool for teamwork and free flow of information about operational programs. A study is presented that positive attitude and natural curiosity is required in SOC work to be able to follow cyberattack trends. Presents top management as the driving force for the development and implementation of the SOC. Process: Presents that fully defined processes are necessary to determine the actions and responsibilities of the members in the SOC. Presents that its essential to note that process factors always depend on the functions, services, and technologies used to establish the SOC Technology: Presented in two perspectives. The first perspective focuses on monitoring, identification, and evidence collection. Vulnerability scanning, penetration testing, and malware analysis are in the second perspective. Publication sees this an additional function that supports the main objectives of the SOC.
43	Building and Securing the Modern Security Operations Center (SOC). Mughal, A. A. (2022)	SOC Management	People: Presents that in the future, collaboration needs between SOC and departments like IT and compliance will increase. Process: Expects that more compliance and regulation requirements will have an affect to SOC as organizations need to abide to stricter security standards. Technology: Predicts that automation and AI will handle increasingly larger portion of the incidents in the future.
46	Rethinking Security Operations Centre Onboarding. Onwubiko, C. (2021)	SOC Management	People: During the onboarding, SOC engages with the business stakeholders and asset owners to understand business requirements for the services that will be monitored by SOC. The unique business drivers for the organization should be a focus for the SOC. Process: Emphasization of the dynamic nature of cybersecurity onboarding as an ongoing process rather than a single, one-time event. New acquired or setup business services need to be monitored and on the other hand monitoring needs to be downsized if services are discontinued. Technology: Presents future state cybersecurity onboarding where cloud-based automation and orchestration is leveraged in cloud hosting environments. Infrastructure as a code and automation is recommended to be used. Onboarding process can be done in a single deployment cycle in code.

ID	Publication	SOC domain relates most	How the publication relates to CTEM PPT properties
54	Cybersecurity Arm Wrestling. Rehman, R. (2019)	SOC Management	People: Utilization of threat modeling to define scope, determine log sources, select appropriate tools and technologies to your SOC. In case of a large organizational environment, priority for SOC building should be given to high-risk businesses. Discusses also creating a SOC Governance Board with relevant stakeholders and creation of policies for SOC and teams that SOC needs to work with. For example, a log collection and incident identification and escalation policies. Process: Publication highlights many processes. For the vulnerability management it makes a point that the organizational program for this can be run by SOC or by a separate team. Regarding patch management, point is made that SOC, for its own infrastructures patching, should follow the organizations patch management process. Technology: Among the essential technologies is mentioned ticketing system and workflow tools.
55	SOC-AM: An Accessible Maturity Model for Security Operation Centers. Revaclier, A. R. (2021)	SOC Management	People: Argues that being able to automate requires working with teams from different domains of the organization. Doing automation might require a periodic meeting where different work efforts are examined to recognize possibilities for automation. Process: Presents that SOCs are used by many organizations in many different forms and it lacks standardization. Technology: Metrics used to identify bottlenecks in operations and used to communicate benefits of the SOC.
56	SOC Service Areas: Identification, Prioritization, and Implementation. Rodman, C. et al. (2024)	SOC Management	People: Presents that security risk assessment should prioritize what services SOC will offer. The risk assessment should identify what security controls are in place and where gaps currently are. Process: Highlights a publication, SOC Critical Function Guide, that states possible SOC service areas of proactive detection, awareness of all IT assets, and vulnerability management. Technology: No direct technological references.

ID	Publication	SOC domain relates most	How the publication relates to CTEM PPT properties
70	Security Operations Center: A Systematic Study and Open Challenges. Vielberth, M. et al. (2020)	SOC Management	People: Points out that an absence of a proper communication platform can reduce the SOC staff interactions. Also, to be able to detect unknown attacks the use of non-security people, like engineers, will become more important in the future. Process: States that clear understanding of SOC processes requires that those can be integrated with organizations other business processes. Technology: Organizations IT and OT environment is increasing in complexity. Situational awareness is becoming harder to maintain.