# Framework for SOC performance metrics and enhancement

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Department of Computing, Faculty of Technology
October 2025
Kari Vahteri

Supervisors:
Hasanov Ismayil
Mohammad Tahir

UNIVERSITY OF TURKU
Department of Computing

Kari Vahteri: Framework for SOC performance metrics and enhancement

Master of Science (Tech) Thesis, 57 p.
Department of Computing, Faculty of Technology
October 2025

---

Cybersecurity has been an important part of all organizations in the past 10 years. In current cyber landscape it is important to be protected from the threat actors and to protect the organization's infrastructure. This is what a Security Operations Centers (SOC) do and it is important to be able to determine how well your SOC is performing.

This thesis examines the performance metrics and indicators currently used to assess the effectiveness of SOCs and how such metrics can support the improvement of SOC performance. Empirical experience suggests that existing methods for measuring SOC effectiveness are inadequate, limiting organizations' ability to determine whether their SOCs truly enhance overall cybersecurity capabilities.

The study applies Design Science methodology, resulting in the development of a framework for selecting appropriate SOC performance metrics. This framework was demonstrated by identifying five metrics that can be applied across different SOC organizations to evaluate both performance levels and effectiveness within various MITRE ATT&CK tactic categories.

Based on the literature review, it was observed that the existing metrics presented in the literature do not provide sufficient information to be applicable across all SOCs. Using the developed framework, the previously proposed metrics were found to be partially inadequate, highlighting the need for more systematic and holistic measurement approaches.

The outcome of this research is a set of five validated performance metrics and a selection framework that enable SOCs to evaluate and compare their performance across organizations. These contributions provide a foundation for the development of future industry standards in SOC performance measurement.

Keywords: SOC, security operations center, security operations center metrics, cyber defense, performance indicator

TURUN YLIOPISTO
Tietotekniikan laitos

Kari Vahteri: Framework for SOC performance metrics and enhancement

Master of Science (Tech) Thesis, 57 s.
Cyber Security
Lokakuu 2025

---

Kyberturvallisuus on ollut tärkeä osa kaikkia organisaatioita viimeisen 10 vuoden aikana. Nykyisessä kyberympäristössä on tärkeää suojautua uhilta ja suojata organisaation infrastruktuuria. Tätä varten on olemassa turvallisuusoperaatiokeskukset (SOC), ja on tärkeää pystyä määrittämään, kuinka hyvin SOC toimii.
Tässä tutkielmassa perehdymme tietoturvavalvomon suorituskyvyn mittaamiseen ja miten näitä metriikoita voidaan hyödyntää tietoturvavalvomon tehokkuuden parantamisessa. Tässä työssä käytetyn kirjallisuuden perusteella voimme todeta nykyiset tietoturvavalvomon tehokkuuden valvontamenetelmät riittämättömiksi, mikä vaikeuttaa organisaatioiden kykyä arvioida, parantaako tietoturvavalvomo todellisuudessa niiden kyberturvallisuuskyvykkyyksiä.
Tutkimusmenetelmänä käytetään Design Science -metodologiaa. Tutkimuksen tuloksena kehitettiin viitekehys, jonka avulla voidaan valita tarkoituksenmukaisia suorituskykymittareita eri tietoturvavalvomoihin. Viitekehystä havainnollistettiin valitsemalla viisi mittaria, joiden avulla arvioitiin tietoturvavalvomon suorituskykyä ja sen kyvykkyyttä eri MITRE ATT&CK -taktiikkojen kategorioissa.
Kirjallisuuskatsauksen perusteella havaittiin, että nykyiset kirjallisuudessa mainitut mittarit eivät tarjoa riittävästi tietoa että niitä pystyttäisiin käyttämään kaikissa tietoturvavalvomoissa. Kehitetyn viitekehyksen avulla aiemmin esitetyt mittarit osoittautuivat osittain puutteellisiksi, ja niiden rinnalle tarvitaan uusia, systemaattisemmin muodostettuja mittareita.
Tutkielman tuloksena syntyneet viisi suorituskykymittaria ja viitekehys tarjoavat käytännöllisen lähtökohdan tietoturvavalvomoiden toiminnan arvioinnille, sekä mahdollisuuden vertailla suorituskykyä eri organisaatioiden välillä. Tutkimus luo siten pohjan tuleville alan standardeille ja jatkotutkimukselle tietoturvavalvomoiden suorituskyvyn mittaamisen kehittämiseksi.

Asiasanat: tietoturvavalvomo, SOC, suorituskyvyn mittaaminen, suorituskykyindikaattori, kyberpuolustus

# Contents


**1 Introduction** **1**

1.1 Research problem . . . . . 2

1.2 Research methodology . . . . . 2

1.3 Research questions . . . . . 3

1.4 Research objectives . . . . . 4

1.5 Structure of the thesis . . . . . 4

**2 SOC and current metrics** **5**

2.1 What is a SOC . . . . . 5

2.1.1 SOC architecture . . . . . 8

2.1.2 SOC Functions . . . . . 9

2.1.3 SOC roles and responsibilities . . . . . 11

2.1.4 Metrics for SOC performance in literature . . . . . 14

2.2 Challenges in SOC performance monitoring . . . . . 17

2.2.1 Measurement challenges . . . . . 18

2.2.2 SOC Analysts and cognitive load . . . . . 20

**3 Proposition of performance metrics and enhancement** **23**

3.1 Metric selection . . . . . 26

3.1.1 MTTD Evaluation . . . . . 26

3.1.2 MTTA Evaluation . . . . . 27

3.1.3 MTTA&A and TTA evaluation . . . . . 28
3.1.4 Incident Response Time evaluation . . . . . 29
3.1.5 MTTR evaluation . . . . . 30
3.1.6 False Positive Rate evaluation . . . . . 31
3.1.7 Cost of an Incident evaluation . . . . . 33
3.1.8 Quality of Analysis evaluation . . . . . 33
3.2 Enhancement propositions . . . . . 34
3.2.1 Tiered vs tierless SOC . . . . . 34
3.2.2 AI Machine learning in enhancing performance . . . . . 37
3.2.3 Security Orchestration, Automation and Response . . . . . 38

**4 Evaluation of proposed SOC metrics 40**
4.1 Evaluation of metrics in a tierless SOC . . . . . 41
4.2 Evaluation of metrics in a tiered SOC . . . . . 44
4.3 Evaluation results . . . . . 47

**5 Discussion 48**
5.1 Metrics and usefulness from the applied study . . . . . 48
5.2 Enhancements from the applied study . . . . . 52

**6 Conclusion 55**
6.1 Research limitations . . . . . 56
6.2 Future work . . . . . 57

**References 58**

# List of Figures

2.1 PPTGC Framework . . . . . 7
2.2 General SIEM architecture . . . . . 8
2.3 SOC Tier model pyramid . . . . . 12

# List of Tables

2.1 SOC Functions . . . . . 11

3.1 Quality criteria for SOC performance metrics . . . . . 24
3.2 Metric validation Table . . . . . 35

4.1 Events Analyzed by Analysts . . . . . 41
4.2 Mean Time To Acknowledge . . . . . 42
4.3 Mean Time To Report . . . . . 42
4.4 Quality of Analysis . . . . . 43
4.5 MITRE Tactics used . . . . . 43
4.6 Tiered SOC Events Analyzed by Analysts . . . . . 44
4.7 Mean Time To Acknowledge in a Tiered SOC . . . . . 45
4.8 Incident Response Time in a Tiered SOC . . . . . 45
4.9 Tiered SOC Mean Time To Report . . . . . 45
4.10 Tiered SOCs Quality of Analysis . . . . . 46
4.11 Tiered SOC MITRE Tactics used . . . . . 46

# Acronyms

**AI** Artificial Intelligence.

**API** Application Programming Interface.

**APTs** Advanced Persistent Threats.

**DFIR** Digital Forensic Incident Response.

**DSRM** Design Science Research Methodology.

**EDR** Endpoint Detection and Response.

**IDS** Intrusion Detection System.

**IoC** Indicators of Compromise.

**KPI** Key Performance Indicator.

**LLM** Large Language Model.

**MTTA** Mean Time to Acknowledge.

**MTTD** Mean Time to Detect.

**MTTR** Mean Time to Respond.

**PPT** People, Process, and Technology.

**PPTGC** People, Process, Technology, Governance, and Compliance.

**SEM** Security Event Management.

**SIEM** Security Information and Event Management.

**SIM** Security Information Management.

**SOAR** Security Automation, Orchestration, and Response.

**SOC** Security Operation Center.

**TTA** Time to Analyze Alert.

**TTPs** Tactics, Techniques and Procedures.

**XDR** Extended detection and response.

# 1 Introduction

In an ever-changing cyber world, it is important for every organization to take care of its cybersecurity. All organizations worldwide require technology to run their own critical services and to provide services to other organizations. The global cybersecurity provider Check Point releases statistics that show how cyberattacks have grown by 30% to 50% every year since 2020 [1] [2]. IBM states that a major trend in the past decade has been the rise of sophisticated ransomware attacks. Other trends that have also been noticed are cloud vulnerability exploitation attacks and business email compromise attacks [3]. NetNordic's Threat Intelligence team has also stated in their report that in 2025 there have been more victims listed by ransomware groups in the first six months than what they observed in all twelve months in 2024 [4]. This kind of statistic shows the need for organizations to be able to keep up with the ever-growing number of cyberattacks. In addition, Advanced Persistent Threats (APTs) pose a serious cybersecurity challenge characterized by stealth, persistence, and significant resource investment by adversaries [5]. Traditional security solutions are not enough against APTs and their sophisticated tactics. This is where Security Operation Center (SOC) steps in. The SOC plays an important role in maintaining organizations cybersecurity. As Mutemwa et al. [6] discuss, the SOC plays a critical role in the cybersecurity strategy of organizations. The main goal of a SOC is to detect, respond, and report security incidents [7]. Organizations may operate their own SOCs or acquire SOC services from an external provider. It

is essential to understand how effectively the SOC detects and responds to security threats, as this capability enables organizations to focus on developing their services and delivering value to customers through their products and offerings. Given the critical role of the SOC within organizational operations, it is necessary to first understand its structure and components. Furthermore, evaluating the performance of the SOC and identifying potential areas for improvement are key to enhancing its overall effectiveness.

## 1.1 Research problem

Since the need for SOCs has been growing, it is important to be able to determine the performance of a SOC. The current state of literature about SOC performance metrics does not provide a clear answer as to which performance metrics should be monitored by internal or external SOCs. Selecting a SOC for the needs of the organization can be difficult, and determining which SOC model would best suit organizations needs is also difficult to select if there are no clear performance metrics which to observe and base the decision on. In the literature today, several different metrics for measuring the effectiveness of SOCs are presented. However, the available information on these metrics is often insufficient. For some of them, it is difficult to determine how the metric should be measured in practice, while others apply only to SOCs that follow specific operational models.

## 1.2 Research methodology

In this thesis, Design Science Research Methodology (DSRM) is used. According to Hevner et al. [8], Design Science Research must contribute to both practical relevance and theoretical knowledge through the design and evaluation of new artifacts. Peffers et al. [9] further define a Design Science Research artifact as the outcome of

an iterative framework consisting of the following steps:

1. **P**roblem identification and motivation
2. **O**bjectives of a solution
3. **D**esign and development
4. **D**emonstration
5. **E**valuation
6. **C**ommunication

In this thesis, the first step is discussed in Chapters 1, 2, and 3. The second and third steps are examined in Chapter 3. Chapter 4 focuses on the fourth step, while the fifth step is addressed in Chapters 5 and 6. The sixth step is considered throughout the thesis as a whole.

The research for the literature review of this thesis was done primarily by using these search engines: google.com, scholar.google.com, utuvolter.fi, jyx.jyu.fi. The main research query parameters were 'SOC', 'Security Operation Center', 'SOC performance', 'Security Operation Center performance', 'SOC metrics', and 'Security operation Center performance metrics'.

## 1.3 Research questions

In this master's thesis the aim is to answer the following four research questions:

1. What are the factors that determine the performance of SOC?
2. What metrics should be collected?
3. What could be improved in metrics?
4. How could the performance of the SOC be improved?

## 1.4 Research objectives

This thesis examines the concept of a SOC and reviews the common performance metrics identified in the literature. The study investigates which of these metrics could be more effectively utilized for SOC performance monitoring. After selecting a set of relevant metrics and identifying additional performance improvements from existing research, these findings are tested in an applied study conducted with a real SOC. The study aims to produce empirical data on the usefulness of the selected metrics and performance enhancements. Finally, the thesis discusses how these improvements could be implemented within SOCs and how they might influence daily operations and processes. The overall objective is to develop a comprehensive framework for SOC performance metrics and improvement.

## 1.5 Structure of the thesis

The structure of this thesis is as follows: The first Chapter, Introduction, discusses the rationale behind the selection of this topic and outlines the research objectives that this study aims to address. Chapter 2 discusses more about what a SOC is and the building blocks of a SOC. After discussing what a SOC is, the current state of performance metrics are discussed, and what issues can be seen in the metrics. Chapter 3 goes over the metric selection framework and which metrics could be included in the applied study. In Chapter 4, the study is conducted, and the data collected from the study is shown. Chapter 5 will discuss the metrics used in the study and how the data collected could be used to improve the performance of a SOC. And in the last Chapter 6 is a conclusion, where the results are discussed and if all of the research questions were answered by this study.

# 2 SOC and current metrics

This chapter examines the concept of a SOC. To determine which metrics should be monitored, it is first necessary to understand what an SOC is and how it operates. The chapter begins with an overview of the typical roles and responsibilities within SOCs, followed by a review of the performance measurements commonly discussed in the existing literature. As no universal framework currently applies to all or even most SOCs, it is essential to identify what aspects of SOC performance can be monitored using the tools currently available. This understanding provides a foundation for developing more effective approaches to performance monitoring in the future.

After establishing an understanding of the current state of most SOCs, this chapter examines the reasons why performance monitoring of SOC analysts has often been insufficient and why it remains challenging to assess their performance effectively. Multiple factors contribute to the complexity of defining an appropriate set of performance metrics. By reviewing the existing literature, the aim is to identify a set of performance metrics that could be applied in most SOCs, if not universally.

## 2.1 What is a SOC

A SOC does not have a universally accepted definition. As noted by Vielberth [10], "The biggest issue is the lack of a precise definition of a SOC and its components. For some researchers, a SOC is solely an entity responsible for monitoring the network.

For others, it is an organizational unit encompassing all security operations, such as incident management and threat intelligence."

Consequently, the term SOC can refer to a wide range of configurations. In some organizations, a SOC may consist of a small team of two to three individuals responsible for information security monitoring, maintenance, and development. In this thesis, however, the focus is on external SOC service providers. According to Nathan [11], such SOCs are typically responsible for detecting security incidents and responding to them through various measures. These service providers generally operate multiple teams, often comprising 5–20 specialists, who work collectively to secure the customer's environment.

In the literature, SOCs are most commonly described using the People, Process, and Technology (PPT) framework [12] [13] [14] [15]. Vielberth [10] extends this model by incorporating Governance and Compliance, thereby forming the PPTGC framework. This expanded framework provides a more comprehensive and comprehensible representation of the SOC structure. Figure 2.1 illustrates how the SOC is composed of People, Process, Technology, Governance, and Compliance, as described by Vielberth et al. [10].

Subsection 2.1.3 provides a more detailed discussion of the People component of the PPTGC framework. The Process component, on the other hand, is vital to SOC operations, as it defines how the SOC functions and manages security events. SOC Processes typically follow established guidelines such as the NIST Computer Security Incident Handling Guide [16]. The Technology part describes the tools that the SOC uses for its operations. The technologies used are different for most SOCs. Governance and Compliance offer a framework that governs people's actions and shapes the development of processes and technologies [10].

In general, external SOC service providers are responsible for monitoring customer environments 24/7 and handling alerts arising from them. The scope of SOC

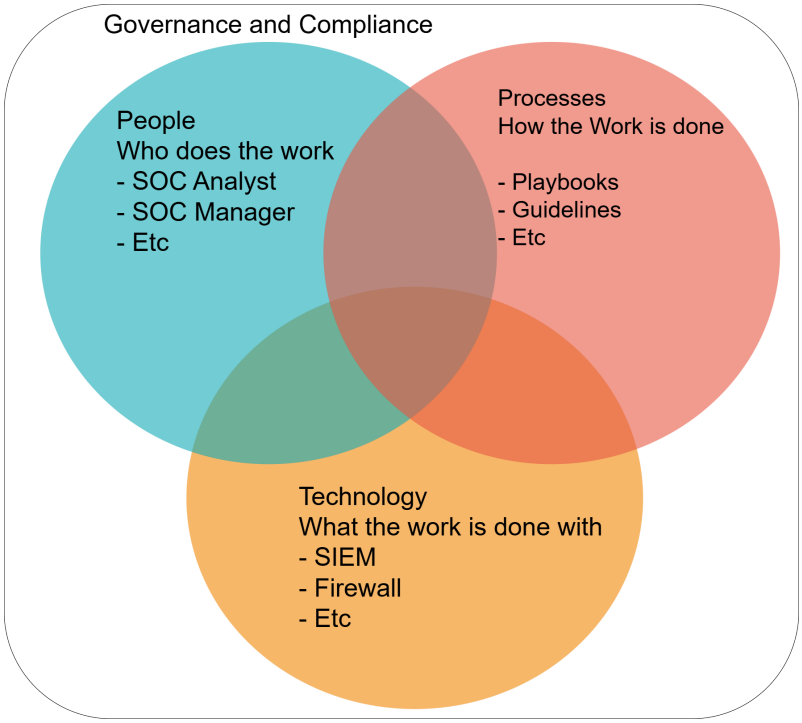


Figure 2.1: PPTGC Framework

monitoring can vary from contract to contract, depending on what services companies have decided to purchase from their SOC service provider. The scope of monitoring affects the sources from which the SOC can receive alerts. However, generally speaking, companies that purchase SOC services have, for example, firewall solutions that provide logs, some kind of Endpoint Detection and Response (EDR) or Extended detection and response (XDR) product that produces logs, network traffic, system logs from servers and endpoints, and other log sources that are all collected to the SOC providers' SIEM [17]. SIEM is an abbreviation of Security Information and Event Management. A SIEM system is a solution that provides real-time analysis of security alerts generated by various hardware and software infrastructures within an organization. It integrates the functions of Security Event Management (SEM) and Security Information Management (SIM) [18]. Figure 2.2 presents a general idea of an SIEM architecture.

When companies look for a SOC provider, they have two options. Organizations

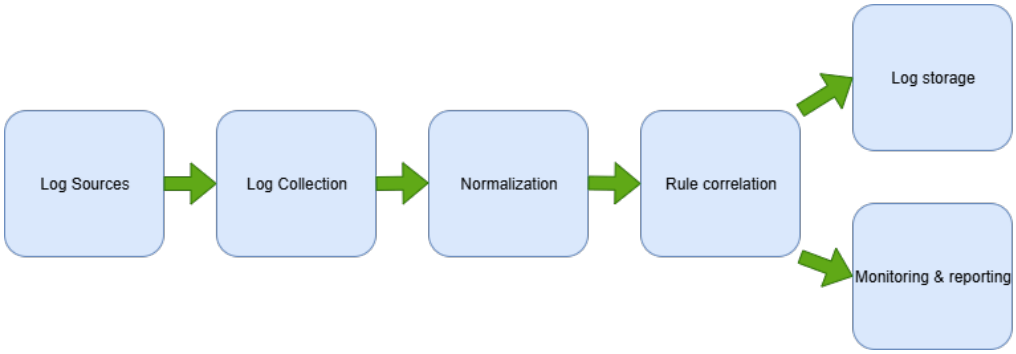


Figure 2.2: General SIEM architecture

can choose to buy a fully managed SOC, which usually handles all security infrastructure. This can include firewalls, EDR/XDR tools, security updates for software, and so forth, and then of course the monitoring and response actions when handling security incidents. The other option is co-managed, where the organization's own security team handles the security infrastructure mostly, and the SOC handles the monitoring and response actions only. The co-managed version does not prevent the SOC from assisting with keeping the security infrastructure up to date, but the main responsibility is on the organization's own security team.

### 2.1.1 SOC architecture

It has been discussed how the SOC can be a team of only a few people or bigger teams of tens of people. The same goes for the SOC architecture. Radu [19] also highlights how there is no "one size fits all" approach to SOC architecture. Vielberth et al. [10] describe how SOC architecture can be centralized, distributed, or decentralized on a high level. In centralized architecture, all of the data from all sources is sent to one centralized SOC. In a distributed architecture, there are multiple SOC subsidiaries that process the logs sent from the organization's environment. This enables the workload of handling the data evenly. And in a decentralized which consists of multiple SOC subsidiaries reporting to one or more central SOCs. Vielberth et al. [10] suspect that this approach is motivated by an attempt to prevent

a single point of failure. Radu [19] conducted a study discussing a typical SOC architecture where segmenting SOC components by functional criteria enables the construction of an architecture characterized by distinct functional layers. These layers are the Generation Layer, Acquisition Layer, Data Manipulation Layer, Output/Presentation Layer, Policies/Procedures. The Generational Layer contains all methods used to collect logs from the environment. The Acquisition Layer is where all of the data collected in the Generation Layer is transferred. This can also include the first round of filtering and prioritization. Data Manipulation Layer is the central component of the SOC from a technical point of view. In this layer, there is SIEM, log management, and other SOC tools reside, and all of the event normalization, filtering, correlation, and analysis is made. Output/Presentation Layer is where SOC tools interface with the human component. The SOC analysts bring value through their own expertise. Policies/Procedures have the organization's policies, procedures, standards, best practices, and guidelines. These interact with the Data Manipulation Layer and Presentation Layer.

### 2.1.2 SOC Functions

When considering the operations of a SOC, its various functions can be categorized into distinct areas. Knerler et al. [20] provide a clear classification of these functions into the following functional categories:

- **I**ncident Triage, Analysis, and Response
- **C**yber Threat Intelligence, Hunting, and Analytics
- **E**xpanded SOC Operations
- **V**ulnerability Management
- **S**OC Tools, Architecture, and Engineering

- **S**ituational Awareness, Communications, and Training
- **L**eadership and Management

The first functional category, Incident Triage, Analysis, and Response, is the primary focus of this thesis. Within this category, there are eight functions. Real-Time Alert Monitoring and Triage at this stage, the SOC analyst does an initial triage and a short analysis of the security incident generated in the SIEM. The second function is Incident Reporting Acceptance. This is the process of reporting the security incidents forward to other teams or receiving reports from multiple sources. The third function that Knerler et al. [20] discusses is Incident Analysis and Investigation. This function is for in-depth analysis of the security incidents and identifying details regarding those incidents. The fourth function is Containment, Eradication, and Recovery. This function involves response actions performed by SOCs to remove the threat actors from the organization's environment. The fifth function is Incident Coordination, where the SOC shares gathered information about an ongoing security incident and coordinates with incident stakeholders or other participant organizations. The sixth function is Forensic Artifact Analysis. This function handles the examination of digital artifacts to get detailed information and to be able to reach a conclusion of the security incident and create a timeline of what has happened. The seventh function is Malware Analysis, which contains examining files and binaries to be able to understand the origin, lineage, behavior, and purpose of the suspected malware samples. And the last and eighth function inside this category is Fly-Away Incident Response. This is the tools and procedures, and practices to quickly react to provide Digital Forensic Incident Response (DFIR) either remotely or onsite.

These functions are at the core of most SOCs. The other function categories also consist of multiple functions that are shown in Table 2.1. It is important to note, as emphasized by Knerler et al. [20], that it is uncommon for a single SOC to cover

Table 2.1: SOC Functions

| Function Category | Function Area |
|---|---|
| Cyber Threat Intelligence, Hunting, and Analytics | Cyber Threat Intelligence Collection, Processing, and Fusion<br>Cyber Threat Intelligence Analysis and Production<br>Cyber Threat Intelligence Sharing and Distribution<br>Threat Hunting<br>Sensor and Analytics Tuning<br>Custom Analytics and Detection Creation<br>Data Science and Machine Learning |
| Expanded SOC Operations | Attack Simulation and Assessments<br>Deception<br>Insider Threat |
| Vulnerability Management | Asset Mapping and Composite Inventory<br>Vulnerability Scanning<br>Vulnerability Assessment<br>Vulnerability Report Intake and Analysis<br>Vulnerability Research, Discovery, and Disclosure<br>Vulnerability Patching and Mitigation |
| SOC Tools, Architecture, and Engineering | Sensing and SOC Enclave Architecture<br>Network Security Capability Engineering and Management<br>Endpoint Security Capability Engineering and Management<br>Cloud Security Capability Engineering and Management<br>Mobile Security Capability Engineering and Management<br>Operational Technology Security Capability Engineering and Management<br>Analytic Platform Engineering and Management<br>SOC Enclave Engineering and Management<br>Custom Capability Development |
| Situational Awareness, Communications, and Training | Situational Awareness and Communications<br>Internal Training and Education<br>External Training and Education<br>Exercises |
| Leadership and Management | SOC Operations Management<br>Strategy, Planning, and Process Improvement<br>Continuity of Operations<br>Metrics |

all of these function categories and functions.

### 2.1.3 SOC roles and responsibilities

As mentioned before, the external SOC service providers usually consist of multiple teams, around 5-20 employees per team. Here is a breakdown of what the common SOC teams are.

Tier 1 analysts: this is the first stepping stone in any SOC. They are entry-level analysts who are responsible for monitoring the SIEM, escalating incidents to T2 or T3 analysts they are incapable of analyzing themselves, or if they believe the alerts contain actual malicious activity [17]. Figure 2.3 shows an illustration of the SOC Tier model.

Tier 2 analysts: Tier 2 Analysts are SOC Analysts who no longer hold the Junior

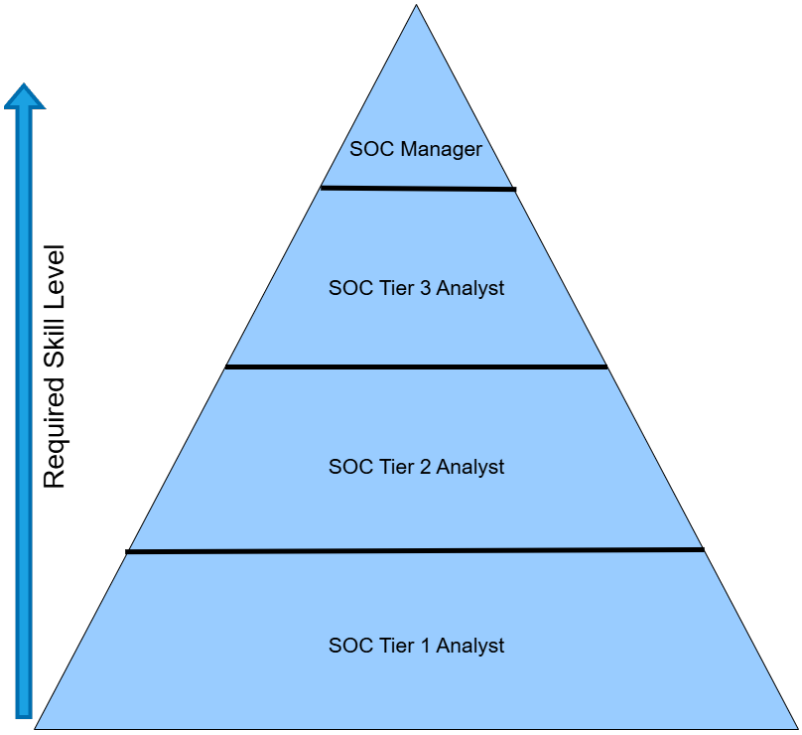


Figure 2.3: SOC Tier model pyramid

title. They are also responsible for analyzing events and assisting T1 analysts with incidents that the T1 analyst has deemed possibly malicious. They have more experience and are expected to do more in-depth analysis of the alerts. They are also expected to be able to collect data from multiple sources to provide more insight on the alerts escalated to them by T1 analysts and to provide information for the organizations on how to contain and recover for any security incident reported by the SOC [10].

Tier 3 analysts: T3 is a senior level position, and they are responsible for multiple different tasks in a SOC. Their main responsibility no longer includes only handling the security events collected in SIEM. T3 personnel focus on threat analysis, malware analysis, and forensic investigation. They are expected to proactively hunt for any threats or vulnerabilities in customer organizations to help organizations with their security posture [10].

Most SOCs also include Threat Intelligence Team, SOC Detection Engineering

Team, and SOC Management. Most of these can be a separate team or a part of the T3 team. Threat Intelligence is responsible for providing critical information for the analysts about current cyber threats and gathering information about threat actors to enrich the alerts generated in SIEM and help analysts understand Tactics, Techniques and Procedures (TTPs) used by threat actors. This helps the SOC to recognize common attack patterns, identify threat actors, and provide information for the organization's security posture [21].

SOC Detection Engineering is responsible for the SOC's capability to identify threats from different data feeds and ensure that the SOC is capable of identifying new and existing threats without generating false-positive alerts which could lead to security incidents being identified incorrectly or it could cause security incidents being not being identified at all [22]. Traditionally, SOCs use a rule-based detection systems based on known signatures and attack patterns, as stated by Khalid [23], which is why they work closely with the Threat Intelligence to provide accurate up to date detection for the SOC.

The purpose of SOC Management is to ensure that teams can effectively handle their respective parts of SOC operations. As Vielberth [10] states, this includes ensuring there are enough employees to handle all of the tasks of SOC, ensuring all SOC members have adequate training, and creating processes. They are also responsible for the financial aspect and report to the SOC organization's Chief Information Security Officer (CISO) or/and other top-level management.

All of these roles are part of the People in the SOC Function shown in Figure 2.1. All of these roles are also part of the Process function shown in Figure 2.1, while the main responsibility for developing and improving processes falls on SOC Management, it is important to involve the personnel working with those processes. The Technology part falls mostly on the SOC management and engineering team. They are responsible for the technologies used in the SOC, such as the SIEM, log

collection technologies, ticketing systems, and so forth [12].

### 2.1.4 Metrics for SOC performance in literature

This section reviews the metrics commonly used to evaluate SOC performance. There is no global framework that would define all of the metrics used, and most SOCs do not openly tell what metrics they are using for the performance measurements [24]. There is more than one method to assess the performance of the SOC [25]. Mughal [26] defines a few measurements that are used by SOCs.

- **M**ean Time to Detect (MTTD). This is the time it takes for the SOC to detect the security incident. MTTD is a commonly used metric for how long a problem exists in different IT systems before it is discovered. It is also a common Key Performance Indicator (KPI) metric for IT incident management, as is described by Courtemanche [27].

- **M**ean Time to Respond (MTTR). MTTR is used to measure how long it takes for a SOC to respond and resolve a security incident. MTTR is also commonly used by different IT solutions, for example, Rumburg [28] describes the usage of MTTR as a service-level metric used by helpdesk to determine how long it takes for a reported incident to be resolved. This is an important metric for customer satisfaction for helpdesks. This also applies to SOCs, since external SOCs communicate with the customer in a similar manner to helpdesks.

- **F**alse Positive Rate. Mughal [26] also discusses how important it is to measure how many of the security incidents reported are False Positive. High False Positive rate shows how the SOC is wasting resources on incidents that are not actually malicious activities, and this takes time from investigating real threats to the organizations.

- **I**ncident Response Time. This metric is used to measure how long it takes for a SOC to respond after detecting the security incident. Shorter Response times could indicate that the SOC is efficient in response actions, which will stop any threat actor more quickly in the environment.

- **C**ompliance. As said by Mughal [26], Compliance measures the SOCs ability to follow common and regulatory industry standards. These regulations include the SOC to be compliant with PCI DSS, HIPAA, NIS2, and GDPR.

- **M**ean Time to Acknowledge (MTTA). The MTTA measures how long it takes from the incident creation time to until a SOC analyst initiates the investigation. Chamkar et al. [29] also discuss MTTA and its usefulness to measure the responsiveness of the SOC team.

- **M**ean Time to Attend and Analyze (MTTA&A). Wickramasinghe [30] also discuss MTTA&A, which starts when the SOC team starts analyzing the security incident and how long it takes for the SOC to correctly acknowledge, analyze the priority, impact, and possible resolution. Wickramasinghe [30] argues that this is a crucial metric to reflect the efficiency and effectiveness of the SOCs processes.

- **C**ost of an Incident. Multiple sources [29] [30] also discuss how Cost of an Incident is a metric to measure how much a single incident costs. This includes direct costs like resources required to investigate and respond. Wickramasinghe [30] also includes indirect costs to this, which includes loss of revenue, damages to the organization's reputation, and costs to ensure a similar incident won't happen again like software or hardware updates.

- **T**ime to Analyze Alert (TTA). Rosso [31] also uses TTA to measure how long it takes from when the incident is created to when the security event has been

analyzed. The TTA metric is also used by Shah et al. [32] when measuring the level of operation effectiveness of a SOC.

- **N**umber of security incidents. This is a SOC metric that is discussed by multiple different authors, such as Salmi [33], Vielberth et al. [10], Agyepong et al. [34], Knerler et al. [20], and many others. This metric is to show how many security incidents/alerts the SOC has to handle on a daily basis. This metric also helps the SOC to determine the required number of analysts to handle the workload.

Agyepong et al. [35] also discuss Quality of Analysis as a performance metric to be followed in SOCs. According to the survey made by Agyepong et al. [35], there are 7 most important factors in the Quality of Analysis. The report should include who, where, when, what, why, how, and recommendation. Who refers to whom the threat actor might be. This includes values like source IP address, usernames, host names, etc. Where refers to the impacted host's IP address, destination port, or location, etc. When refers to when the incident has occurred. What refers the threat actor already knows or what capabilities they have. This can include name of the incident, file names, domain names, asset names, operating systems event IDs, hashes, among other Indicators of Compromise (IoC). Why refers to why the incident the incident is interesting. It can include values like risk, criticality of the system, potential impact, etc. How refers to how the possible threat actor was discovered. This includes method of detection, for example. And the last Recommendations is how the incident should be contained. This can include various actions such as disabling users or isolating devices, etc. All of these metrics are used to measure SOCs performance when dealing with actual alerts and incidents created in the environment.

There is also Adversary emulation, which is discussed into detail by Picus Security [36]. Adversary emulation is used to assess the SOCs coverage against different

types of Tactics, Techniques, and Procedures (TTPs). This kind of assessment provides the SOC with more knowledge against vulnerabilities in the environment and lack of coverage by the SOC. There are different service providers and tools for these kinds of assessments. As mentioned, these assess the SOC coverage against TTPs. The company MITRE has ATT&CK framework used to map different TTPs to known threat actors. The MITRE ATT&CK framework encompasses an extensive list of TTPs. This comprehensive knowledge base is valuable for SOCs in identifying potential gaps in their monitoring capabilities. This framework is acknowledged by all security experts around the world. This framework is also used by security tool providers like Microsoft 365 Defender, to identify all TTPs that can be found from actual alerts and incidents created by the tools to identify the threat actor's behavior.

## 2.2 Challenges in SOC performance monitoring

Because there is no globally acknowledged framework, there are some challenges when it comes to these performance metrics. When looking into the metrics mentioned before, it can be seen that there is a lack of any metrics that could help the SOC management to define actual issues in the SOC teams themselves. The monitoring coverage helps the management to decide where the SOC engineers are needed the most, and they will show if there are some issues with handling the event amounts. It can be seen that many metrics in the literature originate from IT performance metrics, such as MTTR, but their meaning differs in SOCs. For example, Rumburg [28] describes how MTTR is used by helpdesks. To determine useful metrics for SOCs, it is necessary to examine the issues with the current metrics. This thesis will also look into issues that come with selecting a set of performance metrics and how the cognitive load of SOC analysts can be taken into account.

### 2.2.1 Measurement challenges

An examination of the metrics described in Section 2.1.4 reveals many similarities among them. The abbreviations used are often very similar in form, which frequently results in confusion and misinterpretation. Additionally, the overlap of information across these metrics can further contribute to misunderstandings. Chamkar [29] highlights the lack of adequate metrics, noting that some of the metrics discussed in Section 2.1.4 were also proposed by Agyepong [34].

One of these metrics is Cost of an Incident. Chamkar [29] only includes the salary costs of staff involved from detecting the incident to resolving it. This creates an issue in SOC teams. Especially in external SOC operations, the SOC team is formed from multiple tiers of security specialists as discussed in Subsection 2.1.3. A security incident could require assistance from multiple people, and the validation of findings very rarely are solely on one or two security analysts. This complicates cost estimation, as some individuals may be involved in handling a security incident for only five minutes, while others may provide support for several hours. An issue with the metric is that, for example, Wickramasinghe [30] also includes other factors into the Cost of an Incident. Since the metric is not always the same in all use cases, this creates an issue when looking into SOC metrics and when trying to determine the best metrics for the SOC.

MTTD, while it sounds rather simple metric to follow, also has some challenges. Mohammed [37], for example, discusses how this is an important measurement to assess how fast the Intrusion Detection System (IDS) and SIEM identify and alert suspicious behavior. In many security incidents, the first steps of the attack might be completely missed and do not create an alert at all. Or it might be unclear where the first actions regarding the security incident have been. When Mohammed [37] or Mughal [26] discuss MTTD, they talk about single alerts or incidents. This can be misleading when looking at the description they give for the MTTD since it is

only the time it took from specific actions to be noticed by the SOC. This metric can only measure how fast an SOC analyst reacts to a new alert. Not how long it actually takes from actions done by a threat actor to be noticed by the SOC. For that purpose, it does work to some extent, but the definition in most literature is misleading, and when presenting such figures and the MTTD value, the SOC service provider should ensure that the client or other relevant stakeholders clearly understand the meaning and implications of the metric. This also creates an issue that it would mean the same thing as MTTA, depending on the processes of the SOC organization.

When thinking about MTTR, it is also used by different IT solutions, as Rumburg [28] says it is, for example, used by helpdesks to determine how long it takes for an incident to be resolved. In the SOC context, as discussed in Section 2.1, a SOC can be an internal team responsible for the organization's IT security, it can be a fully managed SOC service, or it can be an external SOC service that is responsible for only monitoring the agreed environment. This creates an issue when thinking about MTTR. The measurement works for organizations' internal SOC and fully managed SOC service, but not for the external SOC, which only is responsible for the monitoring. And because this thesis is more focused on the external SOC provider, it is difficult to measure when the security incidents are acted on and resolved, since it is not solely on the SOC to resolve the issue. As said by [29], MTTR can also mean Mean Time to Repair, Mean Time to Recover, Mean Time to Resolve, which all have different descriptions, and this can also lead to confusion and misunderstanding when showing the MTTR metric to other IT organizations.

Many sources, including Mughal [26], discuss how compliance should be a metric for the SOC. This measures that the SOC is following regulatory standards, but how this would be shown as a metric might be a difficult process. There are a lot of different regulations and standards to match depending on where in the world

the SOC is established, which makes it difficult to find a one common metric to be followed by all SOCs. This could be shown in the form of certification, for example, ISO27001, rather than as a performance metric. The compliance part could also be audited, as discussed by Mohammed [37].

MTTA&A and TTA both have the same issue when it comes to following the metric. What is the point when it can be decided that the event has been analyzed by the SOC analyst. This works for the False-Positive events, where it can be tracked when the analyzed event, alert, or incidents status is changed to false-positive. That would determine when the analyst has analyzed it, and it can be measured. Measuring this in True-Positive (TP) cases would be challenging unless a specific mechanism is implemented that requires the analyst to manually update the event status to 'analyzed'. When looking at some of the SIEMs provided by big corporations like Microsoft Sentinel, they do not have such options available. So, the collection of the measurements would have to be built independently to a separate system.

This same issue comes with the Incident Response Time measurement. Common SIEM providers do not have mechanisms to connect when an action is done to an object included in the incident, unless done directly from the incident page in Microsoft Sentinel, for example. That means the measurements would have to be collected, and the metrics would have to be generated in a separate system.

Chapter 3 discusses performance metrics applicable to SOC performance monitoring, as well as the limitations associated with these metrics.

### 2.2.2 SOC Analysts and cognitive load

When discussing SOC analysts' performance metrics, it is also necessary to consider the cognitive load on SOC analysts to ensure that they are capable of maintaining the performance levels being measured. Osholake et al. [38] also discuss in their

article that the primary contributor to a SOC analyst's cognitive load is alert fatigue from false-positive alerts. This analyst burnout from false-positive alerts also lowers the SOC analyst's accuracy when categorizing and analyzing events. In their article, they also discuss a comprehensive analysis of cognitive load factors in cybersecurity decision-making that was written by D'Alessandro and Park. Osholake et al. [38] discuss six primary contributors for cognitive load from D'Alessandro and Parks study:

- **A**lert Volume Overload. This means processing the same false-positive alerts multiple times a day.
- **C**ontext Switching Penalties. This is the cost of switching between tools used in the SOC to monitor, analyze, and report security incidents.
- **T**emporal Pressure Stress. When handling security events time is an important factor and important decisions need to be made fast.
- **U**ncertainty Management. When the threat intelligence is limited or too vague to be used in security analysis.
- **M**ulti-tasking Cognitive Interference. Handling multiple tasks related to security incidents at the same time such as response actions.
- **K**nowledge Integration Complexity. This refers to situations in which an analyst is required to collect information from multiple sources and organize it into a coherent and actionable format to support the investigation of a cybersecurity incident.

In their study, Osholake et al. [38] implemented a framework to recognize and reduce the cognitive load of SOC analysts, and their most substantial reduction came from the false-positive alerts, which reduced on average 52.1%. The reduction of cognitive load also enhanced other parts of the SOC analyst's performance according

to their study, which show the importance of following the cognitive load of SOC analysts in order to improve the overall performance of the SOC. The issue of alert fatigue is also discussed by many other articles, such as [23] [29] [22].

Sundaramurthy et al. [39] also discuss how the cognitive load and Context Switching Penalties on SOC analysts create frustration and increases the turnover rate at the SOC organizations they observed. In their study, they also found out that adequate performance metrics created confidence in the SOC analysts, and they trusted the management's evaluations more.

# 3 Proposition of performance metrics and enhancement

In this chapter, there will be an in-depth review of the metrics selected for use in the practical experiment. Savola [40] presents a model where the most important criteria for the measurements are meaningfulness, measurability, and correctness. Savola's study also discusses usability as a factor that should be considered on a practical level. Poor quality metrics can raise many issues in the SOC, and the metrics can be seen as useless by the SOC [24]. For this reason, all proposed metrics will be evaluated using Savola's [40] model to ensure their usability. Table 3.1 presents the quality criteria for SOC performance metrics based on Savola's model [40]. The same model was applied in Forsberg's thesis [41] when developing technical performance metrics for a SOC.

Following the evaluation of the metrics, additional actions to enhance SOC performance will be examined and analyzed to determine their viability for inclusion in this thesis and the accompanying study conducted with the SOC.

Table 3.1: Quality criteria for SOC performance metrics

| Criteria | Characteristics | Description |
|---|---|---|
| Correctness | Completeness | Each metric should achieve its purpose that is set when constructing the metric. If it is unable to do it without the help of another metric they should be combined. |
| | Objectivity and unbiasedness | The metric should remain the same no matter who is constructing the metrics. The creators opinions should not affect the metric. |
| | Granularity | The metric needs to have appropriate level of detail so it can be linked to SOC function or team. |
| Measurability | Availability | The measurement for the metric needs to be available in a reliable consistent format. |

| | | |
|---|---|---|
| | Reproducibility | The metric must be reproducible in multiple organizations. |
| Meaningfulness | Clarity | The meaning of the metric should not change during its life cycle. |
| | Comparability | The meaning of the constructed metric should remain consistent and support valid comparisons across different SOCs |
| | Ability to show progression | The metric has to show progression of daily activities. |
| Usability | Scalability | The metric should be usable with low or high volumes of measurements. |
| | Controllability | The metric has to stay between the expected values. |
| | Portability | The metric needs to be usable in all SOC organizations regardless of their size. |

## 3.1 Metric selection

First, existing metrics from the literature will be selected for consideration in this thesis. These metrics will then be evaluated using Savola's [40] model to determine whether they meet the criteria outlined in Table 3.1.

### 3.1.1 MTTD Evaluation

The first metric to be discussed is MTTD. When looking at the correctness criteria in the SOC perspective, it does not fulfill the correctness criteria. Wickramasinghe [30] and Mughal [26] argue the importance of MTTD to be able to determine how long it takes for a threat actor to be detected in the environment. Analysis of DFIR reports reveals that the initial actions taken by threat actors are rarely determined with certainty. The reports use wording such as "most likely" when discussing the first actions of the threat actor. In other IT systems and organizations, this is an important KPI, but in SOC, this does not pass the correctness criteria. This could be grouped with other metric, MTTA, or replaced by it completely. When looking at the measurability criteria, there is an issue since MTTD might not be reproduced in other organizations, depending on their logging level and threat detection capabilities. The availability of this metric is not reliable, which is why it also fails the measurability criteria. MTTD as an idea is a meaningful metric. The metric would show impact on daily activities, and it could be used to determine how well the threat detection of the SOC organization works. And if it could be determined for certain that the first actions were done by the threat actor, the metric would pass the clarity and comparability characteristics of the meaningfulness criteria. The usability criteria have the same issue as the meaningfulness criteria. If the initial

actions of threat actors could always be determined, the metric would be applicable across all SOCs regardless of their size, and the volume of measurements would not affect its reliability. For these reasons, however, this metric will not be included in the applied study.

### 3.1.2 MTTA Evaluation

MTTA was mentioned previously how it could perform better than MTTD. Chamkar [29] also discusses the metric's usefulness to measure how quickly the SOC can acknowledge new security incidents. MTTA is directly tied to the SOC analyst's work and how quickly they can start investigating a new incident that has been raised by IDS or SIEM. The metric alone can fulfill the goal of what it is supposed to show, and it is not affected by other sources or people. MTTA is measured from the time the alert or incident was created to when an analyst starts to work on the incident. This can be measured when comparing the timestamps of both actions to determine how long it took for the SOC to acknowledge the incident. The measurement can be reproduced in, if not all, at least most SOCs. For example, all commercial SIEM solution vendors have a way to determine when the incident/alert has been opened by an analyst. MTTA can also measure the daily activities of the SOC and show the progression of how quickly the SOC can start analyzing new security incidents. MTTA as a metric is a commonly used metric for SOC performance, as it can be seen from Subsection 2.1.4, and it can be compared between SOC organizations. MTTA also meets the usability criteria. The metric does not depend on the size or model or any other factor in the SOC organization, and the volume of measurements does not affect it. It can also be presented in visual format for the SOC management for them to be able to see the development of the MTTA metric. Since the MTTA metric fulfills all the criteria of Savola's [40] model, it is possible to determine that MTTA is a valid metric, and it can be used in the applied study.

### 3.1.3 MTTA&A and TTA evaluation

Another metrics that are close to MTTD and MTTA are MTTA&A and TTA. MTTA&A and TTA are rather close to each other. When looking at how Wickramasinghe [30] describes MTTA&A and how Rosso [31] and Shah et al. [32] describe TTA similarities can be seen in these metrics. Both try to determine the effectiveness of the SOC analysis process. When thinking of a metric for determining how long it takes for the SOC to analyze an event, it is an interesting metric to measure the operational performance. The metric is directly tied to the SOC analysts work, and it gives us a clear goal which the metric achieves. Now, the collection of the measurement is not so straightforward. In commercial SIEM tools, there is no clear way to indicate when the analysis has been completed. From where the measurement would be taken could be from the status of the incident, since that is a field that can be found from most, if not all, commercial products. The issue with the status field is that if the status is marked as closed, it can give a false image to other organizations looking at the incidents. Microsoft Sentinel [42] does provide a way of working with tasks to more accurately monitor the TTA if these tasks are set up manually, but similar options are limited in other commercial tools. Since these would have to be manually constructed to the tools at use, also reproducing this metric in other organizations would be challenging. When thinking of TTA and the Meaningfulness criteria, the TTA metric would fulfill the characteristics of the criteria if it could be reliably measured. The Usability criteria would not be fulfilled since the metric would require certain SOC structures and tools, and a service model. For these reasons, TTA or MTTA&A can't be accepted as valid metrics for the applied study.

### 3.1.4 Incident Response Time evaluation

When looking at the metric Incident Response Time, it would also seem like a metric that could be included in the applied study. As Mughal [26] states, with Incident Response Time, it is possible to measure how long from the creation of the incident it takes for the SOC to perform response actions, such as disabling an account or isolating device from the network. With this metric, the goal is to be able to find where response actions have been taken and how long it takes from detections to response. The metric would directly measure the SOC analyst's efficiency to respond to new security incidents. The faster the response time, the less the threat actor can do in the environment [26]. When looking at the measurability criteria and its characteristics, there is an issue when collecting this measurement. The response actions will be logged in if not all at least most commercial SIEM products, such as Microsoft Sentinel for example. But the measurement requires logs from multiple different tools, depending on the organization's environment and SOC model. There could be one tool that handles, for example, device isolation and another tool disables user accounts. This poses an issue that can be resolved by collecting the logs from all different security tools to the SIEM and collecting the timestamps of different actions from there. However, compared to the earlier metrics, this will require the SOC organization to construct adequate logging for this metric to be available. If the metric can be constructed, it will show direct impact of SOC analysts' daily tasks. If the metric was developed further to include the MITRE ATT&CK tactic that is listed in security incidents in most commercial EDR and IDS products, the metric could be more useful in the scope of this thesis. With the MITRE ATT&CK tactic, the management could monitor which tactic would, for example, have the highest Incident Response Time. With such metric, the management could be able to ensure sufficient training for the SOC analysts. Since these measurements are collectible from most commercial security tools, this

metric without the MITRE ATT&CK tactic, would make this a metric that could be used to compare different SOCs, internal or external. Another issue is with the usability criteria. This metric would not pass the portability characteristic of the criteria since it depends on the tools the organization uses and the service model they have with the separate security tools. The other characteristics of usability criteria are fulfilled. Now, as mentioned before, this is a metric that could measure the performance of the response action done by SOC analysts, and it will be included in the applied study, since it does pass most of the criteria characteristics set by Savola [40].

### 3.1.5 MTTR evaluation

In Subsection 2.2.1, it was discussed how MTTR already possesses some challenges when thinking of the metric from the SOC perspective. When looking at the metric with the Savolas [40] model, the correctness criterion already poses an issue. The metric MTTR can't be tied to a single function or team within the SOC, since it depends on the size or source of the incident. Another issue comes with the availability of the metric. To determine when the security incident is resolved is not always dependent on the SOC. In external SOC services, the SOC might not be responsible for resolving the incident and only responsible to report it to the customer. Rumburg [28] regards the metric as important for customer satisfaction in other IT organizations, but the measurement required for the metric might not be collectible for the SOC, and with the difficulty of collecting the measurements when an incident is resolved, it also fails the reproducibility characteristic. Now, if it was possible to reliably collect the metric, it would be capable of showing progression, but it would still not pass the clarity characteristic. The meaning would not remain the same from organization to organization and therefore could not be compared between separate SOC organizations. The SOC organization and service

model would affect if the metric were collectible, so it would not pass the usability criteria. All SOCs are responsible for reporting security incidents to either customer organization with external SOC or to management and other teams in internal SOCs. This metric could be changed a little to pass the metric criteria. If instead of measuring how quickly the SOC responds and resolves a security incident, it would rather measure how long it takes from when the incident analysis starts to when it has been reported onward. Measuring the time from when the analysis of the security incident starts to when it has been reported forward to the customer in external SOCs and to management or other teams in internal SOCs, it could be measured how long it takes for the SOC analysts to analyze and write the initial report of the incident. Again, if it was possible to combine the MITRE ATT&CK tactic to this measurement, the metric would be able to see if certain tactics would take longer to analyze and report, and ensure that the SOC staff has required training on different attack tactics. When looking at MTTR as Mean Time To Report rather than resolve, it would pass the Correctness, Measurability, Meaningfulness, and Usability criteria. When again, removing the MITRE ATT&CK tactic from the measurement, it could also be used to compare between different SOC organizations. This would make the metric valid and usable in the applied study.

### 3.1.6 False Positive Rate evaluation

Another metric that could be used in the applied study is False Positive Rate. When looking at the correctness criteria and its characteristics, there is an issue with this metric. In order for this metric to be used the fulfill the goal of showing how many of the generated alerts are false-positive and show the progress over time to see how the SOC engineering team has been able to reduce the number of false-positive alerts it is also required to have measured the total number of security alerts/incidents. By combining these two into a single metric using the number of alerts/incidents

reported as false positive and the total amount of alerts/incidents in a certain time frame, to determine how many of the incidents that come from IDS or SIEM are false-positive. This would give the SOC engineering team a visibility on which alerts are categorized as false positive and they would be able to develop the threat detection capability of their SOC. Since the metric would include all alerts/incidents created and all alerts/incidents categorized as false-positive the metric would not be impacted by any biases. The amount of alerts can also be collected from all commercial SIEM tools, and all commercial tools also have the ability to categorize alerts/incidents as false-positive. This metric should be available and able to be reproduce, if not in all, at least in most SOC organizations. The only issue with this metric might be the definition of false-positive. In this context, when discussing false positives, it means that the security incident/alert was not malicious activity. Some security providers, such as Microsoft also uses a Benign True Positive [43] when the alert was created, for example, when using an attack tool, but its usage is allowed and acknowledged. The Subsection 2.2.2 also discusses about the cognitive load of SOC analysts, and D'Alessandro and Park [44] also determined that alert volume overload is one of the main contributors of cognitive load. With the False Positive Rate metric, it would be possible to reduce the cognitive load of SOC analysts by reducing the number of alerts that they have to process. The False Positive Rate could also be used to compare different SOCs, not depending on their organizational model in any way. If comparing just a percentage of false-positive alerts from the total amount, it does not depend on the SOC organization. Since the False Positive Rate metric does comply with all of the criteria when the total number of alerts is added to it as a measurement, it can be used in the applied study.

### 3.1.7 Cost of an Incident evaluation

As discussed in Subsection 2.2.1 Cost of an Incident is a difficult metric to use in all SOC organizations. Although many authors like Vielberth et al. [10], Chamkar et al. [29], and Wickramasinghe [30] discuss the importance of the metric, it is a difficult metric to expect from all SOCs. The metric would not be tied to a specific team, and it could be influenced by bias since it could differ from organization to organization from what the costs are made of. In addition, collecting the measurements for the metric would be difficult and impossible for most external SOC providers. For the previously mentioned reasons, the metric could not be reproduced in other organizations either. If it was possible to create the metric, it would fill the Meaningfulness criteria. With the metric, it would be possible to determine the costs for the organization from each incident, and it would be able to show progress over time, and which incidents require more resources from the costs. The Comparability characteristic would also be difficult to fulfill since it depends on the salaries and software and hardware costs that would differ from organization to organization. For these reasons Cost of an Incident is not a valid metric in this thesis, and it won't be used in the applied study.

### 3.1.8 Quality of Analysis evaluation

The last metric to be discussed is Quality of Analysis by Agyepong et al. [35]. According to Agyepong [35], the metric "Quality of Analysis" is measurable as long as the criterion is limited to the fulfillment of the previously discussed seven points, where, when, what, why, how, and recommendation. It is specifically tied to the SOC analysts, and it would fulfill the goal of ensuring that all relevant information is included in the reports to customers, management, or other internal teams. When only ensuring that the seven criteria are met, it is not affected by bias of the person creating the metric. Collecting the metric from the created reports is possible, but

it requires manual labor if not automatized. The metric can be reproduced in any SOC organization, so it does pass the Measurability criteria. With the metric, it would be possible to show the progress, and it is comparable between SOCs. The size or organizational model does not affect the metric at anyway, and volume of measurements does not affect the metric. The only issue is collecting the measurement from the created reports and how the values are presented at the report. The metric meets the criteria for being a valid metric and will be used in the applied study.

After the validation of the common metrics found in the literature, there are five valid metrics for the applied study. In Table 3.2 are listed the valid and invalid metrics with a short description why the metric is valid or invalid in the context of this thesis.

## 3.2 Enhancement propositions

This section discusses potential methods for improving SOC performance and examines how the metrics selected in Section 3.1 can be applied to evaluate whether the implemented improvements achieve the desired outcomes.

### 3.2.1 Tiered vs tierless SOC

In literature, it is much discussed how SOC is constructed of T1, T2, and T3 analysts and how the tiers dictate the analyst's workload. Harris [45] discusses how the concept of tierless SOC can tackle some of the challenges posed by tiered SOC. With tiered SOC, there are known issues in communication, and moving the security incidents from tier to another, and tierless SOC is an option that tries to tackle these challenges. The goal of the tierless SOC is to train the analysts for a wider range of tasks. Harris [45] states in his PhD thesis that the key advantages of a tierless SOC

Table 3.2: Metric validation Table

| Metric | Validation status | Note |
|---|---|---|
| MTTA | Valid metric | Mean Time To Acknowledge is a metric that can be used by most SOCs and valid for our test |
| Incident Response Time | Valid metric | Incident Response Time is a valid metric with little manual work by the SOC |
| False Positive Rate | Valid metric | False Positive Rate is a valid metric to help lower the cognitive load of SOC analysts |
| MTTR | Valid metric | Mean Time to Report has been deemed as a valid metric that can be used by most SOCs |
| Quality of Analysis | Valid metric | Quality of Analysis is deemed as a valid metric when looking at the seven criteria of quality |
| MTTD | Invalid metric | MTTD does not provide accurate enough metric to be considered a valid metric |
| MTTA&A/TTA | Invalid metric | Time To Analysis is a metric which can't be reliably measured and thus is a invalid metric for this thesis |
| Cost of an Incident | Invalid metric | Cost of an Incident is a metric which can't be reliably measured and thus is a invalid metric for this thesis |

are efficiency, improved communication, optimized resource use, and addressing the talent shortage. When thinking of a tierless SOC, it does give the idea that the efficiency might be better since there are less people working on a single security incident, and there is no need to move the events from tier to tier, creating wait time until the next analysts start to work on the security incident. This could also decrease the Incident Response Time metric discussed in Section 3.1. When there are less analysts working on the same security incident, there is less chances for miscommunication. Knerler et al. [20] also discuss what makes a tierless SOC work. They go over how important in a tierless SOC it is to help new staff members with their investigations and how important playbooks are, for example, for a new analyst in a tierless model. With tierless SOCs, the staff needs to be more aware of prioritizing their work, and the management to be more aware how an analyst is dividing their time between all SOC tasks. Knerler et al. [20] states that when a SOC grows in size, it is important to have clear role descriptions, so a single analyst is not responsible for all SOC tasks. Knerler et al. [20] also discusses the importance of work culture where the team needs to act as a team and help each other out, since when the analysts are working on response actions, another might need to take their place doing the event triage. Knerler et al. [20] talks about how choosing a tiered or a tierless model comes down to the following steps.

- **R**espond to all alerts
- **R**espond to alerts in a timely manner
- **I**nvestigate every alert properly
- **G**ive everyone the opportunity to work at their level
- **G**ive everyone the ability to advance
- **M**aximize operations quality and repeatability

For the purposes of this thesis, the applied study involves comparing the selected metrics between a tierless and a tiered SOC. Through this experiment, the impact of each operational model on the chosen metrics can be observed and evaluated.

### 3.2.2 AI Machine learning in enhancing performance

Machine learning and especially Artificial Intelligence (AI) have been discussed more and more in the media and academic reviews in the past years. Li [46] describes AI as follows "Artificial intelligence (AI) is fast-growing branch of computer science that researches and develops theories, methods, techniques, and application systems to simulate, extend, and expand human intelligence.". And when discussing about AI like ChatGPT, those are a type of AI called Large Language Model (LLM). LLMs are AI that is trained to understand and generate human-like text, have contextual awareness, and problem-solving skills. Rafiey et al. [47] discuss in their research how false positive alerts are a burden for the SOC analysts and how LLMs can be used to reduce the false positive rates. Wang et al. [48] proposed a transformer-based framework to reduce false-positive alerts/incidents to help SOC analysts with alert handling. By using advanced ML models, they were able to improve prediction accuracy and lower the cognitive load caused by false positive alerts of SOC analysts. Khayat et al. [49] does discuss the challenges related to the transformer models since it relies on high-quality training data, and it has computational demands. This could limit the use of transformer models in real SOC applications. Oniagbi [22] discusses in their master's thesis how LLMs can be used for the Tier 1 analysts triage process. Yao et al. [50] discuss in their article multiple ways LLMs can be used in cybersecurity and thus by SOCs. They discuss in the article by their words about the good, the bad, and the ugly. For secure coding, Yao et al. [50] go into detail on how LLMs can benefit secure coding practices and how it can be used to detect vulnerable or malicious code, and how LLMs can help to fix the code. From

the SOC perspective, LLMs could be used to detect malicious code in malware analysis, but it could also be used to detect malicious command lines created by malicious software. LLMs could help SOCs to detect malicious activity without the knowledge of every single programming language. Yao et al. [50] also go into detail on how LLMs can be used in cyberattacks such as hardware-level attacks, OS-level attacks, Software-level attacks, Network-level attacks, and User-level attacks. The usage of LLMs can help threat actors with their cyberattacks, but it is also a tool the SOCs can use to detect malicious activity. Many sources like Xu et al. [51] and Rahman [52] discuss the usage of LLMs in threat analysis. LLMs could be used to help analysts understand the security incidents/alerts generated in the SIEM, to help analysts with a lower skill level or who are new to cybersecurity, to understand what is actually happening in the security incidents/alerts.

There are some limitations to how AI and LLMs could be used to help SOC performance. When talking about internal or external SOCs, the data they manage is highly confidential. This means the SOC would require to have an in-house implementation where the AI would not have the possibility to leak the data outside the organization. If using a public AI such as DeepSeek, for example, it creates the possibility of revealing confidential information like happened for DeepSeek in 2025 [53].

For the purpose of this thesis, it is not within the scope of the thesis to implement LLMs to improve SOC performance other than the use of LLMs to help understand the security incident/alert, since this would differ from SOC to SOC how this could and should be implemented and used.

### 3.2.3 Security Orchestration, Automation and Response

Waelchli et al. [54] describe Security Automation, Orchestration, and Response (SOAR) as a technology that enables automation actions for security incidents.

SOAR systems can automatically react to security alerts/incidents by executing playbooks that define the wanted automation actions. Bridges et al. [55] discuss how SOAR tools can be used to automate common manual tasks done by the SOC to improve SOC analysts' efficiency. With the playbooks, things such as password reset, device isolation, and revoking of sessions can be automated to improve Incident Response Time. Bridges et al. [55], in their study of commercial SOAR tools, found that while SOAR tools have the possibility to improve investigation efficiency and reduce content switching, which was one of the six main reasons for cognitive load for analysts according to [38], its success is heavily dependent on the configuration of the SOAR tool. Nandi [56] also discusses how with SOAR tools, it is possible to enhance the detection rules and enrich the data with threat intel, and how with SOAR platforms, anomaly detection can be improved with ML and AI. With SOAR platforms, it is possible to deploy security control also to multiple environments through Application Programming Interface (API), which lessens the manual labor that is needed from the security teams. With SOAR, organizations are also able to address alert fatigue according to Chatterjee [57]. This leads to the conclusion that the use of SOAR tools could be beneficial for SOC performance. However, as their effectiveness is highly dependent on the specific tool and such solutions are not universally available to all SOC providers, SOAR will be excluded from the performance enhancement scope of this thesis.

# 4 Evaluation of proposed SOC metrics

This chapter outlines the methodology for testing the performance metrics and improvements discussed in the preceding chapters. An applied study will be conducted in collaboration with a Finnish SOC provider to validate the practicality and usefulness of the selected metrics.

The applied study examines the selected metrics and the results produced when they are implemented in a real SOC environment. The study consists of two separate sessions in which the performance of SOC analysts is analyzed over twelve-hour periods.

In the initial evaluation, the activities of five analysts are observed over a twelve-hour period while operating under a tierless SOC model. All of the data is anonymized to ensure that neither the SOC provider nor its customers can be identified, and analysts' outputs are pseudonymized to prevent the research data from being linked to any individual analyst.

In the second evaluation, the same five analysts are observed over another twelve-hour period, this time operating under a tiered SOC model.

Table 4.1: Events Analyzed by Analysts

| Analyst | Amount of alerts handled | False Positive amount | True Positive amount |
|---|---|---|---|
| Analyst 1 | 393 | 391 | 2 |
| Analyst 2 | 96 | 95 | 1 |
| Analyst 3 | 64 | 64 | 0 |
| Analyst 4 | 83 | 82 | 1 |
| Analyst 5 | 0 | 0 | 0 |
| Total | 636 | 632 | 4 |

## 4.1 Evaluation of metrics in a tierless SOC

For the first evaluation, the data was collected from the SOC on 2025-09-24 from 07:00 to 19:00 (UTC+3) Finnish time. There are five analysts that work between that time frame. Each individual analyst's metrics are analyzed, and then grouped as a whole to verify if the metrics and the addition of the TTPs provide earlier discussed outcome. Only incident created by SOCs customers EDR and Cloud products are selected for this study in order not to go into the detection capabilities of SOC where the study is conducted. That means that all of the analysts included in this study did T1, T2, and some T3 analysts' responsibilities that were discussed in Subsection 2.1.3. In Table 4.1, it can be seen how many alerts the analyst handled in the given time frame and how many of those alerts were false positives.

From the Table 4.1 it can be observed that in a tierless SOC, the handling of events is not evenly distributed. Some analysts clearly process a significantly higher number of events than others. From Table 4.1, it can be observed that in a tierless SOC, the distribution of event handling is uneven, with some analysts processing a substantially higher number of events than others. Although additional analysis of other tasks performed by the analysts could reveal whether workload distribution is more balanced across different responsibilities, this study focuses exclusively on the previously selected set of metrics.

Based on the collected data, measurements for the False Positive Rate metric were obtained. From this, it is possible to determine that 0.6% of incidents were

Table 4.2: Mean Time To Acknowledge

| Analyst | Amount of alerts handled | MTTA |
|---|---|---|
| Analyst 1 | 393 | 00:18:32 |
| Analyst 2 | 96 | 00:26:55 |
| Analyst 3 | 64 | 00:08:37 |
| Analyst 4 | 83 | 00:15:34 |
| Analyst 5 | 0 | 0 |
| Total | 636 | 00:18:25 |

Table 4.3: Mean Time To Report

| Analyst | Amount of True positive alerts handled | MTTR |
|---|---|---|
| Analyst 1 | 2 | 00:24:00 |
| Analyst 2 | 1 | 00:35:20 |
| Analyst 3 | 0 | 00:08:37 |
| Analyst 4 | 1 | 00:04:18 |
| Analyst 5 | 0 | 0 |
| Total | 4 | 00:18:04 |

actually true positive on the measured time frame.

For the MTTA metric, the duration between the creation of a security incident or alert and the initiation of its analysis was calculated. Table 4.2 presents the MTTA values for each individual analyst as well as for the SOC team as a whole. On average, security incidents or alerts were taken into analysis approximately 18 minutes after their creation.

For the Incident Response Time metric, the analysis focuses on the timestamps indicating when an alert was taken for analysis and the duration between that point and the execution of response actions. As shown in Table 4.1, there were only four instances in which response actions could have been performed, with such actions being required in only one of these cases. In that incident, 55 minutes elapsed between the initial detection and the completion of the response actions.

For MTTR, the time it took from when the analysis started to when it was reported forward. The average MTTR by analyst can be seen in Table 4.3.

Table 4.4 shows that, out of the four analyzed tickets, three met all seven of

Table 4.4: Quality of Analysis

| Ticket | How many of the criteria were fulfilled | How many criteria there were |
|---|---|---|
| Ticket 1 | 7 | 7 |
| Ticket 2 | 7 | 7 |
| Ticket 3 | 7 | 7 |
| Ticket 4 | 6 | 7 |
| Total | 27 | 28 |

Table 4.5: MITRE Tactics used

| MITRE Tactic | Amount of alerts | MTTA | MTTR | False Positive Rate | Incident Response Time |
|---|---|---|---|---|---|
| Reconnaissance | 6 | 00:23:35 | 0 | 100% | 0 |
| Resource Development | 0 | 0 | 0 | 0 | 0 |
| Initial Access | 184 | 00:18:01 | 00:18:04 | 97.8% | 00:53:00 |
| Execution | 82 | 00:20:12 | 0 | 100% | 0 |
| Persistence | 39 | 00:16:02 | 0 | 100% | 0 |
| Privilege Escalation | 23 | 00:22:50 | 0 | 100% | 0 |
| Defense Evasion | 19 | 00:28:30 | 0 | 100% | 0 |
| Credential Access | 97 | 00:15:18 | 0 | 100% | 0 |
| Discovery | 58 | 00:19:05 | 0 | 100% | 0 |
| Lateral Movement | 3 | 00:19:38 | 0 | 100% | 0 |
| Collection | 6 | 00:11:33 | 0 | 100% | 0 |
| Command and Control | 41 | 00:22:25 | 0 | 100% | 0 |
| Exfiltration | 49 | 00:17:37 | 0 | 100% | 0 |
| Impact | 29 | 00:13:58 | 0 | 100% | 0 |
| Total | 636 | 00:18:25 | 00:18:04 | 98.9% | 00:53:00 |

the previously defined Quality of Analysis criteria, while one met six of the seven criteria. The contents of the tickets cannot be disclosed to prevent the compromise of confidential information.

It was possible to determine the MITRE Tactic for all of the events. Table 4.5 presents the distribution of all events across the MITRE ATT&CK tactics.

Events could also be categorized by analyst according to the MITRE tactics. However, since all reported events fall under the Initial Access tactic, further differentiation by analyst and MITRE tactic is not considered necessary at this stage. If there were more results where security events would have fallen under other categories, there could have been a reason to divide all of the events and tactics between each analyst.

Table 4.6: Tiered SOC Events Analyzed by Analysts

| Analyst | Amount of alerts handled | False Positive amount | True Positive amount |
|---|---|---|---|
| T1 Analyst 1 | 62 | 62 | 0 |
| T1 Analyst 2 | 400 | 396 | 4 |
| T1 Analyst 3 | 613 | 610 | 3 |
| T2 Analyst 4 | 17 | 14 | 3 |
| T2 Analyst 5 | 43 | 39 | 4 |
| Total | 1075 | 1120 | 7 |

## 4.2 Evaluation of metrics in a tiered SOC

In the second evaluation, the data was collected from the SOC on 2025-10-01 from 07:00 to 19:00 (UTC+3) Finnish time. This evaluation includes the same five analysts, but they are separated to tiers compared to the first evaluation. The metrics will be analyzed both at the individual analyst level and for the SOC team as a whole to assess whether differences emerge between a tierless and a tiered SOC, and to determine how the implementation of tiers influences each metric. The study used the same 5 Analysts but with a tiered model. Analysts 1, 2, and 3 were working as T1 analysts, and Analysts 4 and 5 were working as T2 analysts.

Table 4.6 presents the number of events analyzed by each analyst, and how many of those events were true and false positive. The Table shows that, even with the tiered model, event distribution is not uniform across all T1 and T2 analysts. During the observed period, a total of 1075 security incidents or alerts were recorded, however, with the tiered model, some events were handled multiple times, resulting in 1128 analyses conducted.

For Mean Time to Acknowledge in the tiered SOC, Table 4.7 presents the MTTA for each individual analyst as well as for the SOC team overall. On average, security incidents and alerts were taken into analysis 11 minutes after their creation in the tiered SOC.

There were 3 incidents that required actions from the SOC, as can be seen in Table 4.8, and the average Incident response time was 41 minutes and 5 seconds,

Table 4.7: Mean Time To Acknowledge in a Tiered SOC

| Analyst | Amount of alerts handled | MTTA |
|---|---|---|
| T1 Analyst 1 | 62 | 00:11:52 |
| T1 Analyst 2 | 400 | 00:17:34 |
| T1 Analyst 3 | 612 | 00:06:58 |
| T2 Analyst 4 | 0 | 0 |
| T2 Analyst 5 | 1 | 00:14:02 |
| Total | 1075 | 00:11:11 |

Table 4.8: Incident Response Time in a Tiered SOC

| Analyst | Incidents handled that require response actions | Incident Response Time |
|---|---|---|
| T1 Analyst 1 | 0 | 0 |
| T1 Analyst 2 | 1 | 0 |
| T1 Analyst 3 | 2 | 0 |
| T2 Analyst 4 | 1 | 00:29:59 |
| T2 Analyst 5 | 2 | 00:46:38 |
| Total | 3 | 00:41:05 |

with the fastest being 29:59 and the slowest was 59:46. The Incident response time was a bit better compared to the tierless SOCs 55 minutes.

The average MTTR by analyst can be seen in Table 4.9. A comparison of MTTR values between the tiered and tierless SOCs reveals a noticeable difference, indicating that it generally takes slightly longer for a tiered SOC to escalate and report these incidents.

Table 4.10 presents the Quality of Analysis metric, showing the extent to which tickets handled in the tiered SOC met the defined criteria. One of the tickets also clearly passed less criteria compared to the others, which could be a result of a

Table 4.9: Tiered SOC Mean Time To Report

| Analyst | Amount of True positive alerts handled | MTTR |
|---|---|---|
| Analyst 1 | 0 | 0 |
| Analyst 2 | 0 | 0 |
| Analyst 3 | 0 | 0 |
| Analyst 4 | 3 | 00:43:41 |
| Analyst 5 | 4 | 00:36:53 |
| Total | 7 | 00:39:48 |

Table 4.10: Tiered SOCs Quality of Analysis

| Ticket | How many of the criteria were fulfilled | How many criteria there were |
|---|---|---|
| Ticket 1 | 4 | 7 |
| Ticket 2 | 7 | 7 |
| Ticket 3 | 7 | 7 |
| Ticket 4 | 7 | 7 |
| Ticket 5 | 7 | 7 |
| Ticket 6 | 7 | 7 |
| Ticket 7 | 7 | 7 |
| Total | 46 | 49 |

Table 4.11: Tiered SOC MITRE Tactics used

| MITRE Tactic | Amount of alerts | MTTA | MTTR | False Positive Rate | Incident Response Time |
|---|---|---|---|---|---|
| Reconnaissance | 12 | 00:10:33 | 0 | 100% | 0 |
| Resource Development | 0 | 0 | 0 | 0 | 0 |
| Initial Access | 284 | 00:12:21 | 00:38:00 | 98.6% | 00:41:05 |
| Execution | 116 | 00:12:26 | 00:53:42 | 99.1% | 0 |
| Persistence | 96 | 00:14:43 | 0 | 100% | 0 |
| Privilege Escalation | 42 | 00:09:14 | 0 | 100% | 0 |
| Defense Evasion | 64 | 00:11:43 | 0 | 100% | 0 |
| Credential Access | 195 | 00:09:17 | 0 | 100% | 0 |
| Discovery | 62 | 00:08:52 | 0 | 100% | 0 |
| Lateral Movement | 2 | 00:14:03 | 0 | 100% | 0 |
| Collection | 25 | 00:07:09 | 00:17:49 | 96% | 0 |
| Command and Control | 19 | 00:05:40 | 00:55:06 | 94.8% | 0 |
| Exfiltration | 85 | 00:09:53 | 0 | 100% | 0 |
| Impact | 23 | 00:11:07 | 0 | 100% | 0 |
| Total | 1075 | 00:11:11 | 00:39:48 | 99.3% | 00:41:05 |

poorly written ticket or a predefined ticket for that specific customer. Because all the data is anonymized, this cannot be investigated further to see why the ticket differentiates from the other tickets so much.

Table 4.11 shows the distribution of all events across the MITRE ATT&CK tactics for the tiered SOC. From all of the events, Initial Access was the most common MITRE tactic, and Credential Access the second most common MITRE tactic. Least observed MITRE tactic was Reconnaissance, which shows how cloud services do not raise events from external network scans.

In the second evaluation, no significant differences are observed when examining the distribution across the MITRE tactics. Some of the data presented was collected automatically, while other portions were manually extracted from the logs. As the

study relied solely on cloud-based data sources, most of the MITRE tactics were already represented within the security incidents and alerts.

## 4.3 Evaluation results

The applied studies were conducted on cloud-based data sources to ensure that the detection capabilities of the SOC where the studies were conducted would not be exposed. The metrics functioned as discussed in the framework for metric selection presented in Chapter 3. The five selected metrics provided visibility into the effectiveness of the SOC in both applied studies conducted with the SOC service provider. Comparing the metrics with the MITRE ATT&CK framework proved effective, as information on tactics was either already present in the events or could be easily added based on the event data. Some values had to be collected manually, as initially anticipated, but all necessary information was obtainable from the logs of each cloud service provider. These metrics can therefore be used to measure the effectiveness of a SOC and to evaluate its performance across different operational areas, as well as in comparison to various MITRE ATT&CK tactics.

# 5 Discussion

This chapter presents the findings from the study described in Chapter 4. First, the discussion focuses on the metrics themselves, evaluating their usefulness and potential applications. Subsequently, differences between the tiered and tierless SOC models are analyzed, followed by a review of additional enhancement proposals identified through the applied study.

## 5.1 Metrics and usefulness from the applied study

The study showed that if a SOC handles events, these metrics can be collected from most, if not all, commercial products. When looking at the MTTA, Chamkar et al. [29] states that this metric can be used to measure the responsiveness of the SOC team. In the first day of the study, the SOC handled 636 events in the twelve hours that the measurements were collected from, and on average, each security incident was taken into analysis by an analyst in 18 minutes after it was raised in the SIEM. And in the second study, it was even lower at 11 minutes. This metric was easy to produce, and there was no outside force that could affect the measurement during the applied study. From this metric, it can be determined how long it takes per analyst to start analyzing the security incidents and see if there is an issue there or if the workload is not applied evenly. The metric is also comparable between different SOCs to determine which SOC could start analyzing events quicker. This is also important since if a threat actor gains access to the environment, it is crucial

to be able to stop them as fast as possible. Based on the literature review and the applied study, this metric can be determined to be a measurement that should be monitored by all SOCs.

MTTR was already an established metric in IT, as discussed in Chapter 2. With the change to Mean Time To Report, the measurements for the metric were easy to collect without any additions to the SOCs processes or tools. This can be seen as a crucial metric for external SOC providers, as was discussed in Subsection 2.1.4. With this metric, the SOC is able to measure how fast they can report any incident to the customer or internally, depending on the organization structure. The lower the MTTR is, the faster the organization can respond to any security incident and mitigate the threat that has been reported. From Chapter 4 it can be stated that there is clearly a difference between the two applied studies, and it is possible to compare the results between different SOCs. What this metric should be will differ between organizations, and for external SOCs, it depends on the contracts what the value of the metric should be. For this study, the metric is valid to measure differences between SOCs and their reporting time.

False Positive Rate was also collectible from both applied studies, but does it provide the value discussed earlier? The metric can be collected and is available from most commercial providers, and in the applied study, there was no need to modify or manually gather these measurements. Examining both applied studies in Chapter 4, the proportion of false positive security incidents and alerts approaches 100%. Mughal et al. [26] note that a high false positive rate is a clear indication that the SOC is expending resources on handling non-malicious incidents and alerts. A difference is observed between the two studies: in the first study, the lower number of incidents to handle resulted in a better MTTR value. However, this improvement may also be attributed to the tierless SOC structure, which does not involve the delays associated with escalating incidents between tiers, as occurs in tiered SOCs.

If the SOC would be able to lower the amount of false positives without affecting its ability to detect and react to security incidents/alerts, this metric can be used in different SOCs and be used to compare which SOC performs better in this category. In addition, lowering the amount of false positives without affecting the ability to detect and respond would lower the analysts cognitive load as discussed by Osholake et al. [38]. In other words, the metric is valid for this study, and it can be used to measure differences between SOCs, but it could be affected by bias. To avoid bias, the metric should be collected from a longer time frame from actual observational data and not base the comparison to a smaller set of observation, like was done with this study.

Unfortunately, in both of the applied studies, there were not enough cases to measure Incident Response Time to compare the two studies. The measurements had to be collected manually, which also makes it more difficult for the metric to be collected for a longer period of time, but the measurements were collectible from all cloud sources used in the applied study. This metric is as important as MTTR, as it allows measurement of the duration during which a threat actor maintained access to the environment before that access was revoked. And as Mughal [26] states, the faster the response time, the less damage the threat actor can do in the environment. For this metric to be used efficiently, there should be tools to collect the measurements automatically, otherwise it will not help the SOC or its managers, since it is too laborious to collect from all security incidents. There was a small difference in the metric between the studies, but since the first study only had one instance where this metric was measured, it is not a reliable metric to determine the difference between the two studies. It only proves that it can be collected, and it can be used by at least most SOCs to compare how quickly the SOC can respond to an incident.

In both studies, there were multiple incidents that were reported forward that

allowed us to measure the Quality of Analysis. This metric is also easy to collect, but depending on the amount of reports, it could be quite labor intensive to do manually, as was done in this study. With this metric, the SOC was able to see which tickets contained all of the necessary information required for the reports receiver to understand the contents of the incident, as was discussed by Agyepong et al. [35]. This also allowed the SOC manager to see if a certain analyst is not getting all the right information to the reports. This allows the manager to discuss with the analyst why there is information missing and train the analysts to improve their report writing skills. To compare this between different SOCs is a possibility, and it could be a percentage of how many of the reports created included all of the seven criteria, rather than a table that was used in the applied study, such as Table 4.4.

Examining the two applied studies and the use of the MITRE ATT&CK matrix for categorizing security incidents provides insight into which tactics were most frequently used in the observed incidents. For example, both of the studies showed how Initial Access tactic was tagged the most in all of the security incidents. This is a great way for an organization to see which tactics are used the most in the environment and think of ways to improve their security posture to avoid any of these incidents to cause damage to the organization. Seeing how Initial Access was the most used tactic, the organization can ensure that they have multi-factor authentication in use or have phishing training for the employees, so they won't be falling for phishing or spear phishing attacks. The rate of false positives on these MITRE tactics also gives the SOC a possibility to see what is causing all of the false positive incidents/alerts. For example, there was a lot of incidents in the category of Credential Access. The SOC can use this information to look into those incidents and see why those are being generated, and is it a configuration issue or something else. For MTTA, there was no clear difference in all of the MITRE

tactics, which leads us to believe that the MITRE tactic is not a factor for MTTA. For MTTR, there are differences between the MITRE tactics. This tells us that the information could be used to train analysts on a single tactic or techniques if they clearly take more time to report forward compared to the other tactics. In this study, for example, the MTTR for Execution and Command and Control tactics was significantly higher than for the other tactics reported. This could show a lack of understanding of how to analyze these events, or a lack of visibility to analyze these events properly, for example. The same goes for the Incident Response time per tactic. If there is a clear difference, it can be used by the SOC and its managers to determine if more training or better tools are required to for the SOC to work more efficiently. This could also show the cognitive load of content switching if response actions done in a certain tool takes longer than with another. This, however, is only an issue in external SOC providers who can have customers using different tools for different response actions. The False Positive Rate can also be useful when divided into the MITRE tactics. For example, from Table 4.11 it can be seen that from 19 incidents with MITRE tactic Command and Control, 94.8% were false positive. That is a much lower rate than when measured from the rest of the MITRE tactics. This is valuable information for the SOC engineering team, who are in charge of the rule development and the detection capabilities of the SOC.

## 5.2 Enhancements from the applied study

This section discusses how SOC performance could be enhanced when looking at the metrics that were used to measure the two applied studies.

For all of the metrics to be collected by all SOC providers, first, they would have to automate several things in order to use the metrics. The Incident Response Time relies on the response actions being logged, collected, and then automated to create a report to see how long it takes in each incident. It is also possible that in some

SOCs, all of these metrics would require such tools to be developed. For the MITRE tactics, it is the same. This information is used in many commercial products, but to use it with the metrics collected would require some tools or processes to be created by the SOC. If the events do not have the information of the MITRE tactic, then that would have to be produced by the SOC. For this, the SOC could use AI and LLMs in order to correlate a MITRE tactic for all of the security incidents.

For the Quality of Analysis, some AI model would have to be used for the measurements to be collected from a large number of reports. With AI, the seven criteria: who, where, when, what, why, how, and recommendation could be automatically collected from the reports, so there would be no need to manually go through each report to determine if the criteria are met.

AI could be used to correlate MITRE tactics and assess the Quality of Analysis, as well as support other functions, such as improving overall reporting. However, the development of such AI models is beyond the scope of this thesis.

When looking at the results of the metrics in Chapter 4, it can be seen that, for example, the Incident Response Time is almost an hour in each of the applied studies. This could be improved with the use of SOAR. As discussed in Subsection 3.2.3, SOAR could be used to automate at least some of the response actions in certain cases. This would lower the cognitive load of SOC analysts when they would not have to switch tools they use so often. SOAR could also be used to close and filter some of the false positive alerts, also lowering the False Positive Rate metric. SOAR could also bring more information to the incidents, which would remove the need to get a separate tool or process to assign each security incident a MITRE tactic.

From the study, there are a few clear differences between Tierless and a Tiered SOC. With Tiered SOC, the MTTA value was clearly lower compared to the Tierless SOC. This was to be expected since there is no possibility that all analysts are

creating reports about security incident, for example. Also, with Tiered SOC, there were three SOC analysts who were going through security incidents as their only task. With Tierless SOC, the SOC analysts could also have other responsibilities than just doing the initial triage on security incidents. The MTTR values also reveal a clear difference between tiered and tierless SOCs. The MTTR value is much lower in the Tierless SOC than it was with the Tiered SOC. There could be multiple reasons for this. One could be that moving the incidents from T1 to T2 takes time, and the T2 does have to do some of the same work that the T1 SOC analyst already did. The Tierless SOC applied study also had much lower security incident/alert rate, which can also contribute to this. One measurement that could have been collected for comparison is how many of the false positive alerts were reported to be filtered or how many the SOC engineering team could look into to avoid similar false positive incidents in the future. How those false positive alerts are reacted to differentiates between SOC organizations, and this is why it could not have been a metric in this thesis. Surprisingly, the Incident Response Time was faster with the Tiered SOC, but this could be because the Tierless SOC study only had one occasion where response actions were done. With the MTTR being significantly lower, the Incident Response Time should have been lower too, since response actions can be done before reporting the incident forward. When and by who these response actions are done does depend on what has been agreed in the contract that the SOC can do. From these two studies, there is no clear indication which model is better, Tiered or Tierless. As Knerler et al. [20] discusses, it depends on the organization which model works the best. Tierless SOC also needs more training compared to Tiered SOC since all analyst needed to have T2 level analyzing skills for the Tierless SOC to work seamlessly.

# 6 Conclusion

The aim of this study was to create a framework for SOC performance monitoring and enhancement. Since the cybersecurity field is developing rapidly and the threat actors are also developing rapidly the need to be able to see if the SOC is performing adequately. In the Introduction Chapter 1, four research questions were stated:

1. What are the factors that determine the performance of SOC?
2. What metrics should be collected?
3. What could be improved in metrics?
4. How could the performance of the SOC be improved?

In Chapter 2, the current factors identified in the literature that determine SOC performance were reviewed. When discussing the operation performance, there are multiple metrics to consider, and for this thesis, four operational metrics were chosen and tested in the applied study. These metrics were MTTA, MTTR, Incident Response Time, and Quality of Analysis.

A fifth metric, False Positive Rate, was also selected, however, this metric reflects technical performance rather than operational performance. This also answers the second research question. For the third research question, it was found that not using the MTTR value as a Mean Time To Resolve but rather as Mean Time to Report serves the SOC more and provides better value for the metric. Using MITRE ATT&CK tactics when discussing the performance metrics helps SOCs gain more knowledge from each metric. And the fourth research question has multiple an-

swers. The applied study examined differences between tierless and tiered SOCs. Additionally, in Chapter 3, the discussion addresses the potential of AI and large language models to enhance SOC performance, as well as the use of SOAR tools. These metrics and the metric selection framework could be used by all SOCs, not depending on the size or organizational model of the SOC. The use of these metrics could also help compare SOCs to each other to help selecting the SOC that best suits the organization's needs.

By developing a framework for SOC performance measurement and improvement, this thesis contributes both to academic understanding and to operational practice. As SOCs continue to face increasingly complex threat landscapes, such structured approaches will be essential in enabling organizations to assess, benchmark, and improve their defensive capabilities.

## 6.1 Research limitations

There were some limitations to this thesis. One of the key limitations is the narrow time frame where the metrics were collected. The collected data is accurate, but the results reveal substantial differences in the selected time frames. To have a better understanding of the differences between some of the metrics and Tiered or Tierless SOC, the time frame should be more than twelve hours. If the data was collected, for example, over a period of months and there were more SOCs monitored, the metrics could show better results. With a study conducted over a longer period of time would also provide more insight into how the performance of the SOC could be improved. Another limitation was the lack of maturity when looking at SOC performance related literature.

## 6.2 Future work

Additional research is needed to really see the differences in the discussed improvement methods and metrics. Studying the metrics further would also provide SOC organizations more performance metrics to measure and help SOCs to also select performance metrics important for a specific model of SOC. There were multiple metrics discussed in this thesis, and some of those metrics require more literature to better understand what the SOCs should measure to benefit from measuring the performance metrics.

Better understanding what makes a SOC successful is needed in the context of cyber defense capabilities. Future studies should aim to determine whether SOCs should primarily operate as reactive units, responding to security incidents as they occur, or whether they should adopt a more proactive and pre-emptive role in preventing such incidents before they materialize. The SOC literature today mostly discusses how SOCs react, but should the literature focus more on preventing security incidents is a matter that needs more research. Addressing this gap could provide valuable insights into how SOCs can be strategically developed to balance reactive and proactive capabilities, thereby enhancing their overall effectiveness and strengthening the organization's cyber resilience.

# References


[1] C. P. Research, *Cyber attacks increased 50% year over year*, Accessed: 2025-09-11, 2021. [Online]. Available: https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/.

[2] C. P. Research, *Check point research reports highest increase of global cyber attacks seen in last two years – a 30% increase in q2 2024 global cyber attacks*, Accessed: 2025-09-11, 2024. [Online]. Available: https://www.vigilance-securitymagazine.com/news/top-categories/case-studies/11879-check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks.

[3] I. X-Force, *A decade of global cyberattacks, and where they left us*, Accessed: 2025-09-11, 2024. [Online]. Available: https://www.ibm.com/think/insights/decade-global-cyberattacks-where-they-left-us.

[4] S. Anttila and N. Samáneh, *Mid-year threat intelligence report 2025*, 2025. [Online]. Available: https://netnordic.fi/insights/mid-year-threat-intelligence-raportti-2025/.

[5] W. Li, "A comparative analysis of advanced persistent threat detection methodologies: A systematic review", *Applied and Computational Engineering*, vol. 165, pp. 102–108, Jul. 2025. DOI: 10.54254/2755-2721/2025.LD24900.

[6] M. Mutemwa, J. Mtsweni, and L. Zimba, "Integrating a security operations centre with an organization's existing procedures, policies and information technology systems", in *2018 International conference on intelligent and innovative computing applications (ICONIC)*, IEEE, 2018, pp. 1–6.

[7] C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, "Automate cybersecurity data triage by leveraging human analysts' cognitive process", in *2016 IEEE 2nd International Conference on big data security on cloud (BigDataSecurity), IEEE International Conference on high performance and smart computing (HPSC), and IEEE International Conference on intelligent data and security (IDS)*, IEEE, 2016, pp. 357–363.

[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research", *MIS quarterly*, pp. 75–105, 2004. [Online]. Available: `http://www.jstor.org/stable/25148625` (visited on 10/26/2025).

[9] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research", *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007. DOI: `10.2753/MIS0742-1222240302`.

[10] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges", *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020. DOI: `10.1109/ACCESS.2020.3045514`.

[11] D. Nathans, "Designing and building a security operations center.", 2014.

[12] C. Onwubiko and K. Ouazzane, "Challenges towards building an effective cyber security operations centre", *CoRR*, vol. abs/2202.03691, 2022. [Online]. Available: `https://arxiv.org/abs/2202.03691`.

[13] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy", in *Proceedings of the*

*International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, London, U.K., Jun. 2015, pp. 1–10.

[14] S. Mansfield-Devine, "Creating security operations centres that work", *Network Security*, vol. 2016, no. 5, pp. 15–18, May 2016. DOI: https://doi.org/10.1016/S1353-4858(16)30049-6.

[15] M. Majid and K. Ariffi, "Success factors for cyber security operation center (soc) establishment", in *Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology (INCITEST)*, Bandung, IN, USA, May 2019, pp. 1–11.

[16] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide: Recommendations of the national institute of standards and technology", National Institute of Standards and Technology, Special Publication 800-61 Revision 2, Aug. 2012. DOI: 10.6028/NIST.SP.800-61r2.

[17] L. Kersten, T. Mulders, E. Zambon, C. Snijders, and L. Allodi, "'give me structure': Synthesis and evaluation of a (network) threat analysis process supporting tier 1 investigations in a security operation center", in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, Anaheim, CA: USENIX Association, Aug. 2023, pp. 97–111, ISBN: 978-1-939133-36-6. [Online]. Available: https://www.usenix.org/conference/soups2023/presentation/kersten.

[18] Fortinet. "What is siem?" Accessed: 2025-08-25. (2023), [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-siem.

[19] S. Radu, "Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models", in *Innovative Security Solutions for Information Technology and Commu-*

*nications*, ser. Lecture Notes in Computer Science, vol. 10006, Cham, Switzerland: Springer, 2016, pp. 248–260.

[20] K. Knerler, I. Parker, and C. Zimmerman. "11 strategies of a world-class cybersecurity operations center". Accessed: 2025-08-26. (2022), [Online]. Available: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.

[21] H. Faheem and M. Molloholli, "Enhancing soc operations with ai-driven predictive analytics and threat intelligence", Dec. 2024. DOI: 10.13140/RG.2.2.12630.15684.

[22] O. Oniagbi, A. Hakkala, and I. Hasanov, "Evaluation of llm agents for the soc tier 1 analyst triage process", M.S. thesis, University of Turku, 2024.

[23] I. Khalid and M. S. Purdie, "Ai-powered soc operations: Revolutionizing cyber security incident response and management", Dec. 2024. DOI: 10.13140/RG.2.2.33339.53287.

[24] F. B. Kokulu, A. Soneji, T. Bao, *et al.*, "Matched and mismatched socs: A qualitative study on security operations center issues", ser. CCS '19, London, United Kingdom: Association for Computing Machinery, 2019, pp. 1955–1970, ISBN: 9781450367479. DOI: 10.1145/3319535.3354239.

[25] Y. Maleh, A. Sahid, A. Ezzati, and M. Belaissaoui, "A capability maturity framework for it security governance in organizations", in *Innovations in Bio-Inspired Computing and Applications*, A. Abraham, A. Haqiq, A. K. Muda, and N. Gandhi, Eds., Cham: Springer International Publishing, 2018, pp. 221–233, ISBN: 978-3-319-76354-5.

[26] A. A. Mughal, "Building and securing the modern security operations center (soc)", *International Journal of Business Intelligence and Big Data Analytics*,

vol. 5, no. 1, pp. 1–15, 2022, Accessed: 2025-08-26. [Online]. Available: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21.

[27] M. Courtemanche. "What is mean time to detect (mttd)?" Accessed: 2025-08-29, TechTarget. (Jun. 2023), [Online]. Available: https://www.techtarget.com/searchitoperations/definition/mean-time-to-detect-MTTD.

[28] J. Rumburg, *Metric of the month: Mean time to resolve*, 2012. [Online]. Available: https://www.thinkhdi.com/~/media/HDICorp/Files/Library-Archive/Insider%20Articles/mean-time-to-resolve.pdf.

[29] S. A. Chamkar, Y. Maleh, and N. Gherabi, "Soc analyst performance metrics: Towards an optimal performance model", *The EDP Audit, Control, and Security Newsletter*, vol. 68, no. 3, pp. 16–29, 2023. DOI: 10.1080/07366981.2023.2259046.

[30] S. Wickramasinghe. "SOC metrics: Security metrics & kpis for measuring soc success". Accessed: 2025-08-29, Splunk. (2025), [Online]. Available: https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html.

[31] M. Rosso, M. Campobasso, G. Gankhuyag, and L. Allodi, "Saibersoc: A methodology and tool for experimenting with security operation centers", *Digital Threats: Research and Practice (DTRAP)*, vol. 3, no. 2, pp. 1–29, 2022.

[32] A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "A methodology to measure and monitor level of operational effectiveness of a csoc", *International Journal of Information Security*, vol. 17, no. 2, pp. 121–134, 2018.

[33] N. Salmi, "Tietoturvallisuuden mittareiden nykytila", 2018.

[34] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Challenges and performance metrics for security operations center analysts: A systematic review", *Journal of Cyber Security Technology*, vol. 4, no. 3, pp. 125–152, 2020.

DOI: 10.1080/23742917.2019.1698178. eprint: https://doi.org/10.1080/23742917.2019.1698178. [Online]. Available: https://doi.org/10.1080/23742917.2019.1698178.

[35] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst", *Computers & Security*, vol. 124, p. 102 959, 2023.

[36] P. Security, *What is adversary emulation?*, Accessed: 2025-08-30, 2023. [Online]. Available: https://www.picussecurity.com/resource/glossary/what-is-adversary-emulation.

[37] A. Mohammed, "Soc audits in action: Best practices for strengthening threat detection and ensuring compliance", *Baltic Journal of Engineering and Technology*, vol. 2, no. 1, pp. 62–69, 2023.

[38] S. F. Osholake, C. Umealajekwu, A. Edohen, A. O. Majekodunmi, and U. Evans-Anoruo, "Human-ai collaborative security operations: Optimizing soc analyst cognitive load through augmented intelligence frameworks", *IRE Journals. https://www. irejournals. com/formatedpaper/1709110. pdf*, 2024. [Online]. Available: https://www.researchgate.net/publication/394123580_Human-AI_Collaborative_Security_Operations_Optimizing_SOC_Analyst_Cognitive_Load_Through_Augmented_Intelligence_Frameworks.

[39] S. C. Sundaramurthy, A. G. Bardas, J. Case, *et al.*, "A human capital model for mitigating security analyst burnout", in *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 2015, pp. 347–359.

[40] R. M. Savola, "Quality of security metrics and measurements", *Computers & Security*, vol. 37, pp. 78–90, 2013. DOI: https://doi.org/10.1016/j.cose.2013.05.002.

[41] J. Forsberg and T. Frantti, "Technical performance metrics of a security operations center", *Computers Security*, vol. 135, p. 103 529, 2023, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103529.

[42] Microsoft Corporation, *Investigate microsoft sentinel incidents in depth in the azure portal*, https://learn.microsoft.com/en-gb/azure/sentinel/investigate-incidents?utm_source=chatgpt.com, Accessed: 2025-09-11, Jan. 2025.

[43] Microsoft. "View and manage security alerts — microsoft defender for identity". Accessed: 2025-09-27. (2025), [Online]. Available: https://learn.microsoft.com/en-us/defender-for-identity/understanding-security-alerts.

[44] R. D'Alessandro and J. H. Park, "Factors contributing to cognitive load in cybersecurity decision-making: A comprehensive framework", *International Journal of Information Security*, vol. 22, no. 4, pp. 445–462, 2023.

[45] D. Harris, "Virtual reality visualisations for cyber security", Ph.D. dissertation, University of South Wales (United Kingdom), 2023. DOI: https://doi.org/10.60485/dent-ys02.

[46] J.-h. Li, "Cyber security meets artificial intelligence: A survey", *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018. DOI: https://doi.org/10.1631/FITEE.1800573.

[47] P. Rafiey and A. Namadchian, "Using llms as ai agents to identify false positive alerts in security operation center", 2024. DOI: https://doi.org/10.21203/rs.3.rs-5420741/v1.

[48] W. Wang, P. Yi, J. Jiang, P. Zhang, and X. Chen, "Transformer-based framework for alert aggregation and attack prediction in a multi-stage attack", *Com-*

*puters & Security*, vol. 136, p. 103 533, 2024. DOI: https://doi.org/10.1016/j.cose.2023.103533.

[49] M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, and H. M. Khater, "Empowering security operation center with artificial intelligence and machine learning–a systematic literature review", *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3532951.

[50] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun, and Y. Zhang, "A survey on large language model (llm) security and privacy: The good, the bad, and the ugly", *High-Confidence Computing*, vol. 4, no. 2, p. 100 211, 2024. DOI: https://doi.org/10.1016/j.hcc.2024.100211.

[51] H. Xu, S. Wang, N. Li, *et al.*, "Large language models for cyber security: A systematic literature review", *arXiv preprint arXiv:2405.04760*, 2024.

[52] M. N. Rahman, T. Mohammad, and S. Virtanen, "Leveraging large language models for network traffic analysis: Design, implementation, and evaluation of an llm-powered system for cyber incident reconstruction", 2024. [Online]. Available: https://www.utupub.fi/handle/10024/179397.

[53] C. M. Alliance. "Deepseek cyber attack: Timeline, impact, and lessons learned". Accessed: 2025-09-21. (Mar. 2025), [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/deepseek-cyber-attack-timeline-impact-and-lessons-learned.

[54] S. Waelchli and Y. Walter, "Reducing the risk of social engineering attacks using soar measures in a real world environment: A case study", *Computers & Security*, vol. 148, p. 104 137, 2025. DOI: https://doi.org/10.1016/j.cose.2024.104137.

[55] R. A. Bridges, A. E. Rice, S. Oesch, *et al.*, "Testing soar tools in use", *Computers & Security*, vol. 129, p. 103 201, 2023. DOI: https://doi.org/10.1016/j.cose.2023.103201.

[56] S. R. Nandi, "Next-generation soar systems for ai-enhanced security automation", *Journal of Computer Science and Technology Studies*, vol. 7, no. 8, pp. 540–546, 2025. DOI: https://doi.org/10.32996/jcsts.2025.7.8.62.

[57] S. Chatterjee, "Using siem and soar for real-time cybersecurity operations in oil and gas", *International journal of innovative research and creative technology*, vol. 6, no. 2, pp. 1–11, 2020. DOI: https://doi.org/10.5281/zenodo.14598693.