Measuring the Performance of a Security Operations Centre (SOC) Analyst: An Industry-Validated Approach Based on Weighted SOC Functions

A thesis submitted in partial fulfilment

of the requirement for the degree of Doctor of Philosophy

Enoch Agyepong

School of Computer Science & Informatics
Cardiff University

June 2023

To my late parents
and my family.

Abstract

Analysts who work in Security Operations Centres (SOCs) play a vital role in helping organisations protect their computer network systems against cyber attacks. It is the responsibility of an analyst to monitor, detect, investigate, and respond to cyber security incidents. It is essential, therefore, for analysts to maintain a high level of human performance because poor performance could negatively impact on the overall efficiency of a SOC.

To manage analysts effectively and efficiently, SOC managers use performance metrics to measure analysts' performance. However, the existing literature indicates that current metrics are inadequate because they overlook the key facets of analysts' work. The literature also reveals a lack of a systematic approach for measuring analysts' performance. Despite these problems, there has been very little effort by cyber security researchers to improve performance measurement methods for analysts.

This study proposes a widely applicable method (referred to as the Security Operations Centre Analyst Assessment Method (SOC-AAM)) for measuring the performance of an analyst using the Design Science Research Process (DSRP). The novelty of the proposed method is that it captures the most common and significant analysts' functions and has the potential to be adopted by SOCs worldwide. The proposed method simplifies the process of measuring analyst performance by consolidating existing assessment methods and providing a new formal method. Additionally, it provides a novel guideline for assessing the quality of incident analysis and the quality of incident report.

The results of an empirical testing and evaluation of the SOC-AAM shows that the SOC-AAM offers a useful, easy-to-use and comprehensive approach to measuring an analyst's performance. The SOC-AAM will facilitate SOC managers in overcoming the limitations of current performance metrics by offering a systematic method for measuring an analyst's performance. It would also help analysts to demonstrate their performance across a variety of functions.

Acknowledgements

First and foremost, I am grateful to Almighty God for giving me the strength to pursue this PhD research. My gratitude and love go to my wife Jemila and my children, Michelle, Michael and Jason, who sacrificed family time to allow me to work on my research.

I want to express my heartfelt appreciation to my academic supervisors, Dr Yulia Cherdantseva and Professor Pete Burnap, who read, scrutinised and provided the guidance which empowered me to complete this work. A special thanks also goes to Dr Philipp Reinecke for his advice during his time at Cardiff University as my second supervisor. In addition, I would like to thank the members of my annual review panel, Dr Sylwia Polberg and Dr Yuhua Li, for their helpful feedback and suggestions.

I am also grateful to my brother, Dr Joseph Baah Agyepong MD, for always being there for me. Many thanks to all my friends, so many of you, especially Dr Ebenezer Paintsil, Adrian Downey and Dr Mike Lakoju for your encouragement and motivation.

I am grateful to all of the SOC experts and industry practitioners who volunteered their time and expertise for the study. Without their assistance, this work would not have been possible.

Finally, I would like to take this opportunity to express my gratitude to Airbus Defence and Space for funding my PhD research.

Contents

List of Figures

List of Tables

List of Acronyms

CIRT Computer Incident Response Team

CSIRT Computer Security Incident Response Team

CSOC Cyber Security Operations Centre

DSR Design Science Research

IDS Intrusion Detection System

IPS Intrusion Prevention System

IS Information System

KPI Key Performance Indicator

MAM Method Adoption Model

MEM Method Evaluation Model

NOC Network Operations Centre

SIEM Security Information and Event Management

SMEs Small and Medium-sized Enterprises

SOC Security Operations Centre

SOC-AAF Security Operations Centre Analyst Assessment Framework

SOC-AAM Security Operations Centre Analyst Assessment Method

Chapter 1

Introduction

1.1 Research Background

Traditionally, many organisations rely only on security defence tools and technologies such as firewalls, Intrusion Detection/Prevention Systems (IDPSs), Virtual Private Networks (VPNs) and anti-virus software to protect their networks and secure their data from cyber attacks [1, 2, 3, 4]. While these security tools and technologies are useful in detecting and preventing certain types of cyber attacks and intrusions [5], colossal and complex cyber attacks against organisations have shown that relying solely on these defensive tools is insufficient to protect an organisation. These tools cannot help an organisation when it comes to dealing with the aftermath of a cyberattack [6, 7, 8, 9]. Chamiekara et al. [10] point out that defensive tools such as firewalls and anti-virus software become less effective once an attacker discovers ways to circumvent these controls. Furthermore, defensive devices themselves are also susceptible to direct attacks and sophisticated evasion techniques [11]. For example, an Intrusion Prevention System (IPS) can be evaded by a more targeted and stealthy attack or lateral movement of malware [6, 12, 13].

To address the aforementioned problems, many organisations are now utilising the services of a Security Operations Centre (SOC) [14, 15, 16, 17]. A SOC comprises people, processes and technology (see Figure 1.1) and plays a vital role in alerting and taking defensive actions for computer security [18, 19, 20].

According to Schinagl et al. [21], owning a SOC is an important status symbol for organisations as it demonstrates their commitment to protecting their data and that of their clients. In the United Kingdom, for example, the National Health Service (NHS) was given £20m by the central government to establish a SOC in response to security weaknesses identified during the WannaCry ransomware outbreak [22]. A publication by Research and Markets [23] on SOCs in 2019 reported that the global SOC market size is expected to grow from USD 372 million in 2019, to an estimated USD 1,137 million by 2024, at a Compound Annual Growth Rate of 25% during the forecast period.

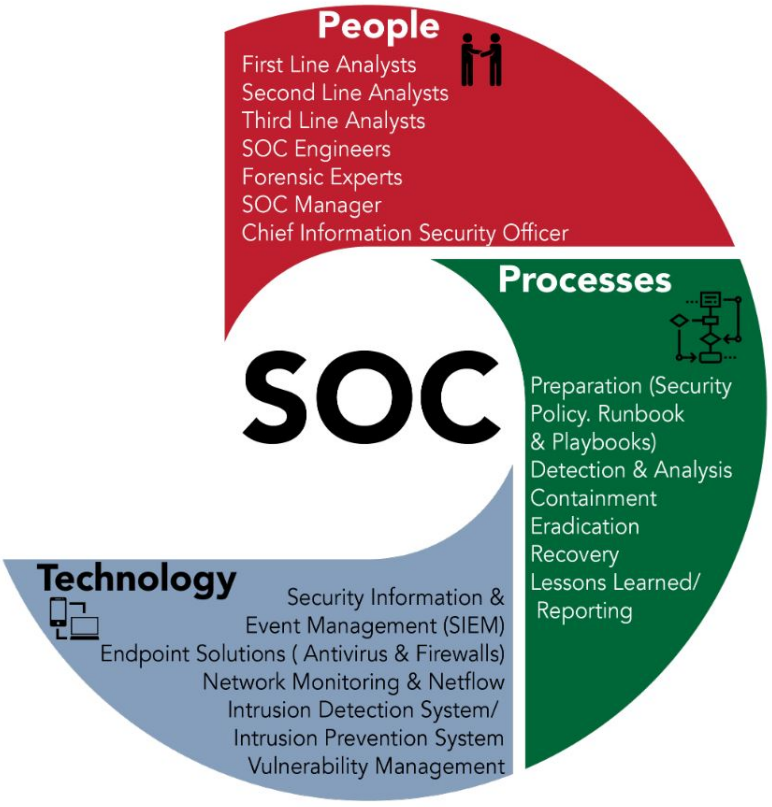

Figure 1.1: Components of a SOC [24] - Image created by author

SOC services cover a wide range of Information Systems and Information Technologies (ISs/ITs) functions, which are explored in greater detail in Chapter 2 of this thesis. SOC services could include the following: helping businesses with meeting compliance and regulatory requirements; dealing with data breaches and internal security policies;

reducing the risk of vulnerabilities in systems and supporting organisations with responding to cyber attacks [25, 26, 27, 28]. SOCs also support businesses to maintain Confidentiality, Integrity and Availability (CIA) of data, as well as playing a central role in the protection of their overall Information Communication Systems (ICS) [21, 29].

While a SOC may offer a range of functions, specific services delivered to individual businesses are often driven by business requirements or clients' expectations [30, 31]. Chamieka et al. [10] state that the functions of a SOC are dependent on the tasks it is being asked to provide by the organisation that owns or buys the SOC services. A SOC can be implemented internally by an organisation or bought as a service from a third-party SOC service provider, commonly referred to as a Managed Security Service Provider (MSSP) [7, 32, 33]. However, most Small and Medium-sized Enterprises (SMEs) are often not in a position to own or operate a SOC as setting up and operating a SOC requires a significant financial investment [34]. SMEs, therefore, rely on an MSSP [28, 35, 36]. A SOC can also be implemented using a hybrid approach by incorporating in-house SOC capability with third-party support [37, 38]. Each approach has its benefits and drawbacks, which are explored in detail in Chapter 2.

1.2 Problem Statement and Motivation for this Study

SOCs rely on security analysts to make sense of collected security logs and data to identify signs of malicious cyber activity and respond appropriately [16, 39]. Analysts also have responsibility to protect a computer network from harm [40, 41]. Furthermore, it is an analyst's responsibility to investigate an alert and decide whether it is a real attack or not [42, 43]. In some SOCs, analysts may also be responsible for fixing vulnerabilities, policy management and the tuning of policies [44, 45]. It is also the responsibility of analysts to maintain deployed security solutions and manage cyber security incidents to reduce damage when it occurs. Axon et al. [46] state that analysts are expected to mitigate malicious network activity. According to Daniel et al. [47], the

ultimate goal of an analyst is to investigate a security incident and write a report that recommends mitigation action/s towards the incident. Figure 1.2 shows the layout of a typical SOC.

Figure 1.2: Layout of a typical SOC [48]

Even though analysts play a vital role in the operation of a SOC, evidence from the literature shows that very few studies have sought to investigate issues affecting SOC analysts [39, 49]. Some scholars opine that the focus of most SOC studies is on technology, with little focus on the human component of a SOC [27, 50, 51]. For example, Alharbi [50] and Mário and Coelho [16] assert that many publications on SOCs focus on technology and exclude people and processes. Yet, as pointed out by Onwubiko [52], analysts (humans) are as important as technology. An effective SOC does not only depend on technical tools and processes but also on human analysts, which makes the assessment of their performance an important issue. Schingal et al. [21] argue that competent analysts are more important than tools and state that SOCs rely on analysts' skills to outsmart sophisticated attackers.

There is only a small number of publications which discuss issues that affect analysts. Chamkar et al. [39] identify challenges faced by SOC analysts and how these impact overall SOC capabilities. Among the problems faced by analysts is the lack of adequate performance metrics [39, 49, 53]. The term 'performance metric' in this context refers to quantitative or qualitative measures or indicators used to assess how well analysts are

performing in their jobs [49]. Even though scholars advocate for the improvement of performance metrics for analysts [54], there is a distinct lack of research on performance metrics for measuring analysts' performance [25, 54].

There is also a lack of research regarding a systematic approach for measuring analysts' performance [54, 55]. The consensus amongst security researchers is that there is a need to improve existing assessment methods to capture the overall performance of an analyst [25, 53, 54, 56, 57].

Although cyber security researchers have suggested a number of metrics for assessing analysts' performance, concerns have been raised about existing evaluation methods for analysts [25, 43, 49, 53, 54, 56, 58]. Firstly, there is concern that existing methods fail to consider the complete range of functions [25]. Secondly, Kokulu et al. [56] assert that current quantitative performance metrics, such as the number of incidents raised by an analyst and the time taken to respond, are ineffective because they do not take into account the severity or priority of alerts processed by analysts. The problem with ignoring alert priority, and measuring performance based on the number of incidents is that some analysts may opt to handle a large number of easy, benign or low priority incidents to look good against such measures [58]. Thirdly, prior research indicates that existing metrics are narrow in focus and discrete and, as such, do not present the entire picture of analysts' efforts and performance within a SOC [25]. The studies [58] and [25] also suggest a lack of a systematic approach for measuring analysts' performance which frustrates both analysts and SOC managers. The evidence from the literature shows that both SOC managers and analysts would benefit from the improvement of performance assessment methods [25, 54].

This leads to the following initial research questions:

(RQ1): *"What metrics exist for measuring analysts' performance in a SOC? What are the strengths and limitations of existing metrics?"*

(RQ2) *"What frameworks and/or models exist for measuring the performance of an*

analyst? Is there a comprehensive framework, model or method for measuring performance?"

(RQ3) *"When evaluating the performance of a SOC analyst, what performance constructs and dimensions need to be considered?"*

The above research questions are important because as stated by Lord Kelvin in 1883: "measurement is knowledge" [59]; unless the performance of analysts are measured, SOC managers cannot identify poor performers.

The research questions - RQ1, RQ2 and RQ3 are investigated and the discussion is presented in Chapter 4.

In order to design a new method for measuring the performance of analysts, it is necessary to understand the functions of analysts. Currently, there is no agreement on what the main functions of analysts are. The existing research on SOCs has not fully investigated the main function of analysts that needs to be considered when assessing their performance. The lack of consensus on analysts' functions impedes the ability to design an effective assessment method. As a part of this study, the main functions of an analyst that need to be considered to assess their performance are investigated and presented in Chapter 6.

Furthermore, there is no agreed-upon set of evaluation criteria. Islam and bin Mohd Rasad [60] state that an effective evaluation system needs a set of well-defined criteria. Without a clear set of evaluation criteria, it would be difficult to measure the performance of an analyst. O'Connell and Choong [61] state that performance metrics must focus on real-life workplace needs and experience. However, this could be problematic because no two SOCs are the same in terms of the functions that they offer; thus, the functions of analysts vary from one SOC to another [21, 51, 52]. To that end, this study seeks to use existing SOC frameworks to understand the operation of a SOC and utilise them as the basis for developing a new approach for measuring the performance of an analyst. This leads to the following research questions:

(RQ4) *"What frameworks exist for understanding the functions of a SOC and how could these frameworks be leveraged to design an approach for measuring the performance of an analyst?"*

(RQ5) *"What are the challenges to devising effective performance metrics for SOC analysts?"*

(RQ6) *"How could the performance of an analyst be measured in a systematic manner addressing the drawbacks of existing methods?"*

Whereas the research questions RQ4 and RQ5 are investigated and presented in Chapter 5, Chapter 6 presents the discussion on RQ6.

1.2.1 Research Aim and Objectives

The overall aim of this research is to develop a widely applicable approach for measuring the performance of a SOC analyst. In fulfilling this aim, the objectives listed below are considered necessary to be achieved in line with the research question. While a research question is a specific concern that has to be answered on the basis of research findings, research objectives are specific actions or activities that will be taken to answer the research questions [62, 63]. The objectives listed below are mapped to the six research questions presented above.

The objectives of this project are as follows:

- **Objective 1:** To investigate existing metrics for assessing the performance of a SOC analyst and their limitations (RQ1);
- **Objective 2:** To investigate existing frameworks and/or models for assessing the performance of a SOC analyst (RQ2);
- **Objective 3:** To investigate human performance constructs and dimensions for assessing an analyst's performance (RQ3);

- **Objective 4:** To investigate existing SOC frameworks and how it could be used to design a new method for measuring an analyst's performance (RQ4);
- **Objective 5:** To investigate the challenges to designing metrics for assessing an analyst's performance (RQ5);
- **Objective 6:** To build and evaluate a new systematic method for measuring the performance of an analyst (RQ6).

1.2.2 Proposition and Hypotheses

This study uses a mixed-method approach and draws on both qualitative and quantitative research strategies. Using a mixed-method approach offers numerous benefits, such as triangulation and comprehensiveness, which increase the validity and academic rigour of this research [64]. A qualitative research strategy is used to establish a detailed description of an analyst's function from the perspective of SOC experts and also to solicit their opinion on how performance should be measured. As a part of the qualitative inquiry strategy, a proposition is devised to derive the solution to the research objectives [65, 66]. A proposition, like a hypothesis, denotes an educated guess or a possible answer to a research question or specific scientific question. However, whereas a hypothesis (which is typically used in quantitative research) is testable and measurable, a proposition shows the links between concepts [67]. A proposition relies on reasoned assumptions and existing correlative evidence [67]. To complement the qualitative approach, a quantitative research strategy involving the use of a questionnaire and hypothesis testing was used in this study to evaluate the proposed approach for measuring the performance of an analyst.

In this thesis, the Security Operations Centre Analyst Assessment Method (SOC-AAM) is proposed addressing Objective 4. The proposition is as follows:

The SOC-AAM is a comprehensive method for assessing the performance of a SOC

analyst, which provides a better coverage of the functions of an analyst than other existing methods.

Further, it is hypothesised that:

1. The SOC-AAM is an easy to use and a useful method for measuring the performance of an analyst $(H.a_1)$.
2. SOC managers and analysts will use the SOC-AAM in future $(H.a_2)$.
3. SOC managers and analysts would perceive the SOC-AAM as a complete method for measuring the performance of an analyst $(H.a_3)$.

1.3 Thesis Contributions

The contributions of this research to the body of knowledge are as follows:

(1) The first contribution of this study is the formalisation of the main functions of a SOC analyst. As a part of this research, the functions of a SOC and metrics for measuring an analyst's performance were identified and presented in a SOC conceptual framework. This contribution was published in the *2020 International Conference on Cyber Security and Protection of Digital Services (IEEE Conference Proceedings)* [55] as reported under Section 1.5. The SOC conceptual framework is used to propose the Security Operations Centre Analysts Assessment Framework (SOC-AAF), which focuses on the primary functions of an analyst and the metrics that could be used to capture their performance. The SOC-AAF served as the building block of the SOC-AAM. The SOC conceptual framework and the SOC-AAF are grounded in the existing frameworks and capture the most common and significant aspects of analysts' operations. They also consolidate and expand the existing SOC frameworks and metrics to provide a comprehensive approach for measuring an analyst's performance.

(2) The second contribution of this thesis is the SOC-AAM, which integrates the SOC-AAF with the principles of the Analytic Hierarchy Process (AHP), a mathematical model for combining subjective and objective criteria as part of a multi-criteria decision-making process. The SOC-AAM provides a formal approach for systematically measuring the performance of an analyst. To the best of the researcher's knowledge, this is the first empirical study to re-contextualise the AHP into a SOC setting and specifically as the basis for measuring performance. By drawing on the AHP framework, SOC managers and stakeholders are presented with a rigorous method [68] for solving the current problems detailed in section 1.2. The SOC-AAM offers a new approach to measuring performance, allowing SOC managers and stakeholders to aggregate, quantify and measure the efforts of analysts in a systematic manner, considering several functions that are expected of an analyst. The SOC-AAM is a comprehensive and adaptable approach. It is comprehensive because it covers all the main functions expected of an analyst [55]. The SOC-AAM is adaptable because it could be used to suit each specific SOC as per the functions and services offered by a SOC. This contribution was published in the *Computers & Security* journal [69] as reported under Section 1.5.

(3) The third contribution of this research is the provision of novel guidelines or indicators for assessing the quality of incident analysis and the quality of incident report as a part of the performance assessment process. To the best of the researcher's knowledge, this is the first study to work collaboratively with industry experts to propose formal guidelines for assessing the quality of incident analysis and report. This guideline will help both experienced and novice analysts who suffer from the complexities of security incident analysis tasks [2]. This contribution was published in [69] as reported under Section 1.5.

(4) The fourth contribution of this study is in providing a detailed insight into the operations of SOCs and analysts for cyber security researchers who have no direct access to SOCs and SOC experts. Aspects of this contribution have been published in the *Journal of Cyber Security Technology* [49] and as a book chapter in *Modern*

Theories and Practices for Cyber Ethics and Security Compliance [24] as reported under Section 1.5.

Additionally, cyber security researchers and system designers could draw on the artefacts proposed in this study [69] when designing systems for SOCs to facilitate the evaluation of performance. For example, security monitoring tools such as Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDSs) typically used by analysts could be designed to incorporate some of the performance metrics proposed in this study.

1.4 Thesis Structure

This thesis is divided into eight chapters as is shown in Figure 1.3.

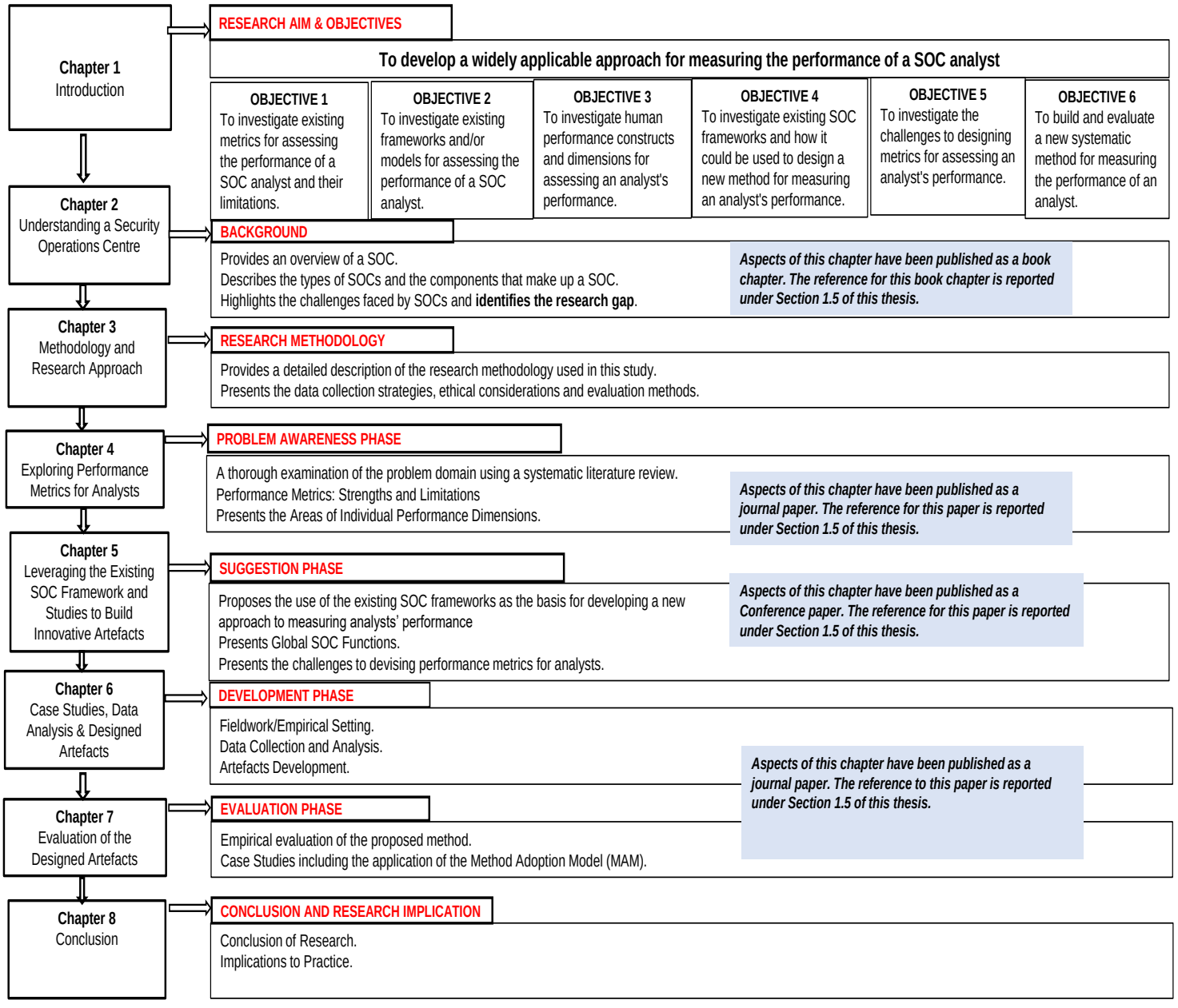

Figure 1.3: Structure of the Thesis

Below presents a summary of the content of each chapter:

- **Chapter 1 - Introduction**

  This chapter provides background information on the research domain, problem statement and the motivation for the study. It also presents the research aim and objectives along with the study's proposition and hypothesis. Additionally, the contributions of this research are presented.

- **Chapter 2 - Understanding a Security Operations Centre**

  This chapter presents an in-depth exploration of SOCs to understand their origin, structure and operations. It discusses the types of SOCs and highlights the strengths and limitations of the different types of SOCs as well as the roles within a SOC. The chapter also explores the challenges faced by a SOC **which led to the identification of the research gap**.

- **Chapter 3 - Methodology and Research Approach**

  This chapter presents a detailed description of the methodology used in this study to achieve the research aim and objectives. Furthermore, it provides an account of the adopted research paradigm, the data collection methods and justification for the selected methods, the selection of study participants, the data analysis techniques, validation techniques and the ethical considerations.

- **Chapter 4 - Exploring Performance Metrics for SOC Analysts**

  This chapters presents the first step of the adopted DSR process by exploring the problem area. The chapter investigates the existing metrics for assessing the performance of an analyst using a systematic literature review. A discussion of the existing frameworks and models for measuring the performance of an analyst is presented. This chapter also presents the problems with existing assessment methods, as discussed by various scholars. The chapter also presents individual work performance constructs and dimensions in a SOC.

- **Chapter 5 - Leveraging the Existing SOC Frameworks and Studies to Build Innovative Artefacts**

  This chapter presents the suggestion phase of the DSR process. It discusses the existing SOC frameworks and models and utilises them as the foundation for developing an approach for measuring the performance of an analyst. This chapter also presents the challenges to improving assessment methods for SOC analysts.

- **Chapter 6 - Case Studies, Data Analysis and Designed Artefacts**

  This chapter presents the outcome of the empirical case studies and fieldwork conducted in this research. The artefacts developed in this project are presented in this chapter. These are constructs, framework, method and instantiation.

- **Chapter 7 - Evaluation of the Designed Artefacts**

  This chapter presents the evaluation of the artefacts developed in Chapter 6. The chapter starts with a discussion and a reflection on how this research adheres to the guidelines for conducting good design science research. This is followed by the presentation of the evaluation of the conceptual framework which contains constructs, the SOC-AAF and the SOC-AAM using SOC experts.

- **Chapter 8 - Conclusion**

  This chapter presents the summary of this study, key achievements and outcomes. Additionally, the chapter presents the study's implications for both academic research and practice, as well as the limitations and avenues for future research.

1.5 Publications and Talks

The publications listed below were produced as a direct result of this research.

Journal Papers

(1) Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2023). A Systematic Method for Measuring the Performance of a Cyber Security Operations Centre Analyst. *Computers & Security*, 124, 102959.

This paper introduces the SOC-AAM, a key contribution of this thesis. The SOC-AAM provides a method for measuring a SOC analyst's performance in a comprehensive and systematic manner, taking into account the level of importance of each function. Chapter 6 draws on this publication and discusses the SOC-AAM in greater detail.

(2) Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2020). "Challenges and performance metrics for security operations center analysts: a systematic review," *Journal of Cyber Security Technology*, *4*(3) pp.125-152.

This paper provides a comprehensive overview of the challenges faced by SOC analysts and of the metrics suggested in the literature for measuring analysts' performance. Additionally, the paper discusses the drawbacks of the existing metrics and argues for improvement of measurement methods for analysts. Chapter 2 presents the challenges discussed in this publication. Furthermore, in Chapter 4, the existing performance metrics presented in this paper are also discussed.

Conference Paper

(3) Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P., "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst," In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Dublin: IEEE, 2020, pp. 1-8.

This paper presents a framework consisting of the core functions of analysts and metrics

that can be used to measure the performance of analysts. This study analysed the functions of a SOC described in multiple sources of literature and engaged with several analysts and SOC managers from different industries using qualitative semi-structured interviews in order to identify the functions and the metrics. The functions and metrics are used in this thesis to develop a systematic approach for measuring the performance of a SOC analyst. Chapter 6 draws on this publication and discusses the SOC Conceptual framework in greater detail.

Book Chapter

(4) Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2020). Cyber Security Operations Centre Concepts and Implementation. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 88-104). IGI Global.

This book chapter contains a discussion on the basics one needs to know about SOCs. The authors introduce readers and IT professionals who are unfamiliar with SOCs to SOC concepts, types of SOC implementation, the functions and services offered by SOCs, as well as some of the challenges a SOC faces. The content of this book chapter is extended and discussed in detail in Chapter 2 of this thesis.

Talks and Collaboration

The content of this thesis has been actively communicated to various individuals and groups. The SOC conceptual framework containing the primary functions of an analyst and the metrics for measuring their performance were presented to researchers and practitioners at the 2020 Cyber Science Conference, who recognised the subject's importance and the contribution of the work.

As a part of this PhD, aspects of this thesis were also communicated to other researchers and students at a number of poster day events held at Cardiff University.

Five guest lectures were also presented to MSc and undergraduate students specialising in Cyber Security at the School of Computer Science and Information, Cardiff University using some of the content from this thesis. Also, aspects of this thesis were shared

through presentations to cyber security graduate students undertaking internships at the Airbus site in Newport, UK.

1.6 Chapter Summary - Conclusion

This chapter introduced the research study and provided the basis upon which the rest of the thesis is constructed. The research problem and research questions were identified. Furthermore, the study's research aim and objectives, together with the proposition and hypothesis, were introduced. In addition, the contribution of the thesis was presented. The next chapter provides an in-depth exposition of the background information on SOCs and establishes the context underlying the research. Additionally, it identifies and justifies the rationale behind conducting this research.

Chapter 2

Understanding a Security Operations Centre

2.1 Introduction

This chapter investigates the origin and operations of SOCs. It discusses the different types of SOC implementation, and the roles within a SOC. Also, the challenges faced by SOCs are presented along with the identified research gap, which justifies the need for this study.

2.2 State of the Art on SOCs

The last two decades have seen a surge in the number of SOC publications [49], with some cyber security conferences specifically calling for research work on issues pertaining to SOCs [70], signifying the importance of this topic.

The growing interest in SOCs is driven by the need to both understand SOCs and improve SOC operations. Table 2.1 presents an overview of the studies on SOCs that served as an inspiration for this research. The research reported in the papers presented in Table 2.1 covers a wide spectrum of SOC topics. A key lesson from the studies in Table 2.1 is that SOC studies span multiple dimensions, perspectives and facets.

Table 2.1: Existing research on SOCs that served as inspiration for this study.

Author(s)	Purpose of Research	Methodology	Outcome
Jacobs et al. [30]	Design a classification and a rating scheme for SOCs and a metric for measuring the effectiveness of a SOC.	Systems Engineering Best Practices.	A model for measuring the effectiveness of a SOC based on maturity levels and capability.
Schinagl et al. [21]	Design a framework for building a SOC and a method for measuring the effectiveness of the protection provided by the SOC.	A case study	A model for building a SOC and an assessment method for assessing the protection offered by the SOC.
Onwubiko [52]	Proposes a framework for CSOCs. Summarises the benefits and challenges of operating a CSOC.	Not Specified.	Designs a CSOC strategy and maps it to Her Majesty's Government (HMG) Protective Monitoring Control.

Table 2.1 – continued from previous page

Author(s)	Purpose of Research	Methodology	Outcome
Sundaramuthy et al. [58]	Investigate factors that lead to SOC analyst burnout.	Anthropology	Reports on the need for a balance between human and technological aspects of SOC operations to achieve continuous SOC improvement.
Sundaramurthy et al. [25]	Investigate how to mitigate burnout phenomena among SOC analysts.	Anthropology Grounded Theory	Proposes a model for understanding burnout phenomenon among analysts. Identifies a number of metrics for evaluating analysts' performance.

Table 2.1 – continued from previous page

Author(s)	Purpose of Research	Methodology	Outcome
Miloslavskaya [37]	Propose a SOC classification. Outlines the mission and function of a SOC.	Literature review and survey of existing works on SOCs.	Identifies the mission and functions of SOCs. Proposes key indicators of IS incidents in IoT infrastructure along with SOC classifications.
Sundaramurthy et al. [54]	Explore the role of a SOC and the functions of analysts.	Anthropology	Identify SOC structures and various metrics for assessing analysts' performance.
Alharbi [50]	Formulate an up-to-date definition of a SOC and identifies the essential attributes of a SOC.	Design Science Research	Proposes an artefact for measuring the maturity level of a SOC.

Table 2.1 – continued from previous page

Author(s)	Purpose of Research	Methodology	Outcome
Feng at al. [42]	Develop a user-centric machine learning framework for SOCs.	A case Study	Designs an automatic system to generate a risk score of user activity on the network and present it to the SOC analyst. An analyst can then use the score to prioritise the work.
Majid and Ariffi [27]	Highlight the importance of people, processes and technology factors in establishing a SOC.	Literature Review	Present the key factors that should be taken into consideration to ensure the success of a SOC. These include: top management support, sufficient monetary budget, clear business strategy, environment and physical space.

Table 2.1 – continued from previous page

Author(s)	Purpose of Research	Methodology	Outcome
Mutewa et al. [71]	Examine the challenges of integrating a newly developed SOC into an organisation's existing IT environment.	Discussion Paper	Reports that the three SOC components (people, processes and technology) must be fully integrated and aligned to an organisation's existing resources and processes in order for an organisation to fully realise the potential benefit of a SOC.
Onwubiko and Ouazzane [72]	The aim of the authors was to provide a comprehensive, actionable and adaptable playbook that cyber incident responders and managers can use when handling and managing a cyber security incident.	Application of Modelling technique	Propose a model that can be used to systematically and consistently manage cyber security incidents through the development of a playbook known as SOTER.

2.3 The Paradigm of a SOC

The concept of a SOC has been defined by different writers in different ways. For example, Schingal et al. [21] define a SOC as *a centralised unit within an organisation that assists the organisation in addressing cyber threats, security monitoring, forensic investigation, and incident management*. On the other hand, Onwubiko [52] defines a SOC as *a team of skilled IT professionals operating with defined processes, and supported by technology, to monitor an organisation's network infrastructure and to improve their cyber security posture*. Vielberth et al. [57] define a SOC as *an organisational unit operating at the heart of all security operations supporting an organisation to detect, analyse and respond to cybersecurity threats and incidents using people, processes and technology*.

While researchers have put forward various definitions of a SOC, the consensus amongst scholars is that a SOC functions through the harmonisation of people, processes and technology in order to protect an organisation from cyber criminal activities. Researchers emphasise that the three components: people, processes and technology need to be balanced as they work together to enable organisations to defend their networks against cyber attacks [27, 73].

The evidence from the literature reveals that some researchers refer to a SOC by other names, such as an Information Security Operations Centre (ISOC); Information Technology Operations Centre (ITOC); and Security Intelligence Centre (SIC) [57, 74, 75, 76]. However, these terms are less commonly used by scholars in comparison to the term 'SOC'. There are also other terms usually associated with SOCs that have a completely different objective to a SOC. For example, the terms Computer Security Incident Response Team (CSIRT) or Computer Incident Response Team (CIRT) are often used by some writers to denote a SOC [6, 57, 77]. However, a CSIRT or CIRT is

not a SOC, and as such, these terms must not be used interchangeably [6, 50]. Aijaz [6] points out that a SOC usually works in partnership with a CSIRT; a CSIRT is a subset of a SOC and relies on incident handlers to conduct more detailed investigations and post-incident management activities [78]. Thus, it is not the function of a CSIRT to monitor an organisation's network.

A Network Operations Centre (NOC) is also another term that is often associated with a SOC [56, 57, 79, 80]. This is because a NOC also uses people, processes and technology to monitor an organisation's network infrastructure for performance-related issues [20, 52]. However, there is a distinction between a NOC and a SOC. NOCs deal with network performance issues and the management of network systems [81, 82]. Shahjee and Ware [20] state that a NOC is also known as a "network management center." They further explain that a NOC is a centralised location where network operation and management are exercised over the organization infrastructure. Active monitoring of an enterprise network with the view of detecting intrusion and cyber-threats typically falls outside a NOC's remit [52].

In this thesis, the above definitions of a SOC are adapted and a SOC is defined as *a centralised unit composed of technically qualified people who use defined processes, tools, and technology to identify, detect, and respond to cyber incidents and threats faced by organisations*.

2.3.1 Evolution of SOCs

Since its inception in the 1970s, there have been six different SOC generations [83, 84]. The first-generation SOCs were purposely built for the defence of government agencies [84]. HP [83] states that the first-generation SOCs were often understaffed and relied on emerging technologies such as firewalls and anti-virus to fend off would-be attackers. These SOCs were primarily used for intelligence gathering and managing IT security risks [26]. They also tended to be reactive and relied on signature-based solutions

to detect signs of malicious activity against the organisation [85]. In essence, first-generation SOCs were set up to provide a formalised approach to monitoring and managing governmental and enterprise business IT assets and aimed to detect low impact malicious code [84, 86]. Extant literature suggests that this initial concept of monitoring the network remains to date [52]. Table 2.2 on page 28 presents a summary of the evolution of SOCs and associated timeline.

Advances in technology and the increase in cyber attacks during the mid-1990s resulted in the birth of the second-generation (2G) SOCs. This period was marked by the introduction of vulnerability tracking systems and formalised system patching (2013) [86]. Commercial companies began to offer security-monitoring solutions to paying customers in what is known as a Managed Security Service Provider (MSSP). Compared to the first-generation SOCs, the second-generation SOCs saw a surge in the number of defensive security tools as attackers adopted more sophisticated attack methods [84]. Furthermore, devices such as vulnerability scanners, Intrusion Detection System (IDS) and Security Information and Event Management (SIEM) became available [85]. The introduction of a SIEM was the beginning of using a central repository for correlating different security events into a single system [79].

According to HP, financially-driven attacks between 2002 and 2006 led to the development of the third-generation (3G) SOCs. The 3G SOCs focused on three key areas: security monitoring, response and threat intelligence [83]. This era saw the maturity of SOC services, the birth of the United States - Computer Emergency Response Team (US-CERT) and the Payment Card Industry Data Security Standard (PCI-DSS) [83, 86]. Regulatory requirements such as the PCI-DSS mandated vendors to keep security and data protection standards to deal with fraudulent transactions. Also, regulatory requirements led many organisations to take security, and the protection of their network, much more seriously. HP claims that between the years 2007-2012, businesses noticed that intrusion was inevitable; despite the numerous preventative measures, there was a need for improving 3G SOCs. This need led to the birth of the fourth-generation

(4G) SOCs. Fourth-generation SOCs existed in an era characterised by hacktivism and Advanced Persistent Threats (APT). Under the 4G SOCs, businesses began to shift their attention from detection and prevention to Data Loss Prevention (DLP), detection and containment. Cyber attacks were also directed towards individuals, in addition to organisations.

The use of big data concepts and intelligence-driven methodologies resulted in the emergence of the fifth-generation (5G) SOCs to improve defences against cyber attacks [83]. Under 5G SOCs, organisations also rely on information sharing to detect previously unknown attacks. 5G SOCs, are more efficient, adaptive and automate many of the manual activities carried out by SOC analysts.

Taslet security [84] mentions the rise of the sixth-generation SOCs in what they refer to as NG-SOC. The evolution of digitisation and disruption of technologies such as IoT attacks have led to further improvement of SOC operations to deal with these emerging problems [84]. Indeed, it could be argued that SOCs will undergo a further transformation as existing technologies and processes are likely to become less effective once attackers find new and innovative ways to bypass them. Furthermore, the industry is now beginning to see new technologies such as Endpoint Detection and Response (EDR) and Security Orchestration and Automating Response [39]. Table 2.2 summarises the evolution of SOCs as outlined above.

Table 2.2: SOC Evolution: 1st Generation to 6th Generation

Generation	**Characteristics**
1st Generation SOC (1975-1995)	Decentralised logging. Limited visibility of the network. Reactive/Incident-based. Focus on minimising the impact of malicious code. Limited tools - mainly firewalls and anti-viruses.
2nd Generation SOC (1996-2001)	Centralised logging; 24/7 monitoring; faster response time. High visibility of the network. Emergence of MSSP. Multiple ranges of tools in comparison to the first generation. Tools included: vulnerability scanners, Intrusion Detection/Prevention Systems (IDPS), Security Information and Event Management (SIEM).
3rd Generation SOC (2001-2006)	Implements anomaly detection strategies. Includes data loss prevention strategies. Focus on finding Botnets. Uses Threat Intelligence (TI).
4th Generation SOC (2007-2012)	Introduces prevention strategies. Focuses on Advanced Persistent Threats (APTs). Implements data exfiltration techniques. Focus on containment strategies to stop the spread of threats.
5th Generation SOC (2013-2015)	Uses big data analysis and intelligence-driven methods to detect unknown attacks. More efficient and adaptive because of the range of tools available to the analyst. Proactive hunting. Automates many manual processes, such as log analysis.
6th Generation SOC (2016- till date)	Focus on addressing attacks against IoT devices. Uses Artificial Intelligence (AI) and Machine Learning (ML) algorithms to monitor data. Focus on faster adaptation to the dynamic changes in business and attack vector changes.

2.4 Types of SOC Implementation

Scholars usually suggest three kinds of SOC implementation [7, 24, 30, 45, 74]: in-house (internal SOC); outsourced (external SOC); or hybrid (Table 2.3). Organisations need to carefully review these options before choosing a particular type, as they all have advantages and disadvantages. An in-house SOC is part of the organisation it is defending and, as such, is managed internally by the organisation [56]. It is often set up by an organisation that wants to avoid outsourcing their SOC services for various reasons (such as concerns relating to potential data loss and risk to losing sensitive information [74]). Miloslavkaya [37] explains that an in-house SOC will have a dedicated internal team of experts who are better placed to understand the overall architecture of a company's network than a MSSP, who may have limited knowledge of the network. This, she argues, is essential during a detailed investigation into an incident. An in-house SOC can be tailored to precise business requirements and is expected to be more efficient and effective than an MSSP because it uses the organisation's own processes [37]. However, the cost of building and maintaining an in-house SOC is an expensive venture for most small to medium-sized organisations [10, 28, 87]. Another downside is that an in-house SOC comes with the financial burden of having to recruit and train SOC analysts to the levels of expertise required to work in a SOC. There is also the need for a periodic refresh of hardware and technology to keep up with emerging threats. Therefore, Jacobs et al. [30] suggest that there is no guarantee of a return on investment (ROI) for an in-house SOC.

Many SMEs may not be in the position to build and maintain their own SOC due to the huge financial cost involved [16, 24, 88]. These organisations may opt to outsource the monitoring of their network to a MSSP at a controlled cost [56, 87]. Miloslavkaya [37] states that MSSPs are generally cheaper than setting up an in-house SOC. This view is consistent to that of Jacob et al. [30]. Outsourcing a SOC means that the MSSP handles the monitoring and response to cyber incidents [16, 38]. Organisations using an MSSP will have a Service Level Agreement (SLA) regarding what is expected from the SOC

[89]. A major benefit of using an MSSP is that it brings transparency. According to Miloslavkaya [37], an MSSP may be unbiased as they are not part of the organisational structure. However, there is some inherent risk when using an MSSP, which is it centres around allowing external/third-party entities to handle the organisation's data. MSSPs are often multi-tenanted, which can also mean that the intelligence gathered from one organisation may be used to improve services for other customers [90]. However, data handed over to MSSPs can be mishandled or mismanaged. Nonetheless, contractual agreements will often outline the consequences of issues such as data mishandling.

A hybrid SOC combines the capabilities of an in-house SOC and an outsource SOC. It therefore draws on the strengths and weaknesses of both in-house and outsourced [74]. For example, under a hybrid setup, an organisation may decide to maintain their security logs and conduct analytics in-house but then draw on a third party's services to provide them with support in specialised areas such as Threat Intelligence [74]. Table 2.3 on page 31 shows the three main types of SOCs outlined above.

Table 2.3: Three Types of SOCs

Criteria	**In-house**	**Outsourced (MSSP)**	**Hybrid**
People (Skills Availability)	The organisation needs to recruit and maintain a team of skilled staff. A limited number of skilled professionals.	MSSP will have a pool of staff and resources to address the needs of their clients. They still have the challenge of maintaining skilled staff.	Hybrid SOC offers the middle ground. An organisation can maintain a relatively small number of staff knowing that they can rely on the experts from outside to assist when needed.
Security Processes	Businesses can design and tailor their internal processes.	Processes used for one client may be used to solve a problem for another client.	Businesses design their in-house processes but have the flexibility of drawing on the tactics and processes of a third party.

Table 2.3 – continued from previous page

Criteria	**In-house**	**Outsourced (MSSP)**	**Hybrid**
Technology	The organisation owns the SOC infrastructure and associated software. Hardware needs a periodic refresh and staff training; this leads to a high running cost.	The cost of buying assets is expensive, however, an MSSP can offset this cost by having several clients.	Businesses can reduce the cost of having to invest in expensive tools. Businesses can draw on the tools and techniques of the MSSP.
Financial cost	High initial cost to set up and there are no guarantees on ROI [30].	Initial cost is typically low because the MSSP can leverage vendor infrastructure.	Organisations can reduce the initial investment by outsourcing aspects of their operations to third parties.

2.5 Roles within a SOC

Onwubiko and Ouazzane [38] identify security analysts (also known as SOC analysts or analysts), SOC engineers, SOC managers and a Chief Information Security Officer (CISO) as the roles within a SOC. The titles - security analyst, analyst, and SOC analyst

are used interchangeably in this thesis. SOCs need highly competent cyber security professionals with good technical knowledge and experience; Shah et al. [91] state that SOCs need to be adequately staffed with competent analysts to ensure that their operations run smoothly.

Schinagl et al. [21] argue that the people working in the SOC are the most crucial component of a SOC as they monitor the network to look for signs of attacks or potential threats. Without people, the functions of a SOC will not be realised [92]. People are needed to make informed decisions on threats and to manage and maintain the deployed technical solutions. According to Jànos and Dai [92], there are three different analysts' roles in SOCs (first, second and third level analysts), but they explain that these three roles are often blurred and are not entirely separate. These levels are also reported in [36]. Shah et al. [91] also identify three types of roles in a SOC and categorise them as junior, intermediate and senior levels. The evidence from the literature shows that first-line analysts are often the juniors, followed by the second-line who are the intermediate and lastly, the third-line analysts who are considered the seniors [24, 93].

In [94], security analysts and incident responders are identified as the two key roles in a SOC. While the former has the primary responsibility of monitoring, detecting and triaging cyber security incidents, the latter deals with a deeper analysis of suspicious security events [42]. Incident handlers are often found within Computer Security Incident Response Teams (CSIRT) and have a primary duty of deep investigation post-incidents [92], actively seeking to understand the root cause of an incident. In addition to SOC analysts and incident handlers, the SysAdmin, Audit, Network and Security (SANS) Institute [95] report on other roles, such as SOC subject matter experts, threat hunters and SOC managers.

SOC analysts are usually at the front-line in terms of monitoring and responding to any immediate threats [51, 95]. SOC analysts are qualified IT professionals who monitor and analyse all activities on an enterprise network using packet capture and analysis tools. SOC analysts are first in line to respond to cyber incidents that an organisation

may face. They are central to detecting incidents and investigating what is happening on a network, regardless of the tools in use [80].

SOCs typically operate using a three-tiered structure to perform specific tasks [54, 96, 97, 98]. The tiers that are generally used are tier 1 team, tier 2 team, and tier 3 team [28]. Analysts are often split into tiers depending on their role within the organisation, their responsibilities and set of daily tasks. Analysts in the same tier are typically expected to carry out similar duties. A detailed descriptions of the three tiers are presented in Section 2.5.1 to 2.5.3. Moreover, there are also cyber security engineers (also referred to as SOC engineers) working alongside analysts [79]. SOC engineers are responsible for hardware and software support [17]. Axon et al. [46] state that SOC engineers are responsible for maintaining the SOC infrastructure. SOC analysts and engineers report to a SOC manager, who in turn reports directly to the Chief Information Officer (CIO), or Chief Information Security Officer (CISO), depending on the nature and size of the organisation [21].

2.5.1 Tier One Team

Analysts operating at this tier are also known as 1st line analysts or level 1 analysts. According to Winterborn [9], level 1 analysts are usually junior analysts. They are typically graduates or those new to the cyber industry. The level 1 analysts are typically the least experienced analysts [79]. However, they are at the front line of all initial investigations [97]. Level 1 analysts are expected to carry out the initial triage of all security events and alerts that indicate a potential security incident, and they usually deal with the majority of all incidents [57, 97, 99]. An alert is a notification from a computer system. In [72], an alert is deemed as an incident if it poses threats. In other words, an incident is an alert that is not part of standard operations or normal expected activity and could cause loss or harm.

Level 1 analysts are responsible for attending to most phone calls and emails directed

to the SOC. They are also responsible for monitoring incident queues for the SOC and raising incidents on events that require investigation. They manage reported incidents, update the incident(s) tickets with any progress and finally, they resolve and close incident(s) tickets once it is determined that the incident does not pose a threat or upon the implementation of mitigation actions [56].

Upon the notification of an alert, a level 1 analyst will qualify and verify alerts to determine their seriousness, and validity [99]. They will also carry out triage to ascertain whether the detection is a genuine security incident. If the alert is found to be a 'false alarm' (also known as a 'false positive') the analyst will tune the monitoring system. For example, an IDS can be configured to ignore an alert that is routinely deemed as a false positive [52]. A level 1 analyst would be expected to report on a false positive, make a recommendation regarding why it was a false positive, and create a knowledge base for that alert. If not, the alert would be promoted to an incident, and a ticket would be created to record the relevant information. The level of response to a security incident is determined by its severity; severity levels will be pre-agreed with the customer, depending on the impact on operations and infrastructure criticality [72]. Level 1 analysts will escalate incidents they cannot resolve to tier two [57, 97].

2.5.2 Tier Two Team

Analysts operating at this tier are known as 2nd line analysts or level 2 analysts. Level 2 analysts are expected to conduct an in-depth analysis of incidents escalated to them by analysts operating in the tier one team [28, 97, 98]. Once they receive an incident, they are responsible for its management until it is closed or escalated to tier three [56]. A level 2 analyst will consider incidents, their potential impact and remediation actions within the context of a customer's business activities [28]. In-house, knowledge-based articles containing detailed records of historical incidents and specific actions that were performed to address the incidents are used to support level 2 analysts [97]. Analysts operating at this level may create a strategy for containment and recovery when there

is an incident. Where necessary, a level 2 analyst will escalate an incident to a level 3 team [57].

Depending on the nature of the organisation, a level 2 analyst may have responsibilities such as signature tuning, writing or amending existing use cases [56]. It is pertinent to note that, in some organisations, the role of the first and second-line analysts are blurred, and the two teams, therefore, perform similar activities [17, 96].

2.5.3 Tier Three Team

Analysts within this tier are referred to as 3rd line or level 3 analysts. They are generally expected to possess and demonstrate a higher level of competence within the domain of cyber security than analysts at level 1 and 2 [57]. Level 3 analysts often have an in-depth knowledge and skills set [56]. According to Winterborn [9], level 3 analysts are the subject matter experts of technical issues pertaining to the SOC. Third line analysts deal with the most complex incidents [56], and will often deal with fewer incidents overall (because the majority of incidents will be dealt with by first and second line analysts [93]). The day-to-day role of members within tier-three includes: management of incidents escalated by the 2nd line team, sharing, managing and dealing with threat intelligence. 3rd line analysts will also have the responsibilities of writing signatures and creating use cases; altering security policies on security solutions such as firewalls, intrusion detection and prevention systems; and in some cases acting as consultants to SOC managers [93]. 3rd line analysts will engage with vendors when the need arises to seek additional technical support for the SOC.

Figure 2.1 illustrates the three tier hierarchical structure and typical responsibilities of an analyst operating under each tier.

Despite the tiers, it is important to point out that some SOCs do not use a tiered structure and have a single role for all analysts [43, 96]. Alharbi (2020) states that a SOC can be implemented as a flat or multi-layer structure when it comes to the operations of an

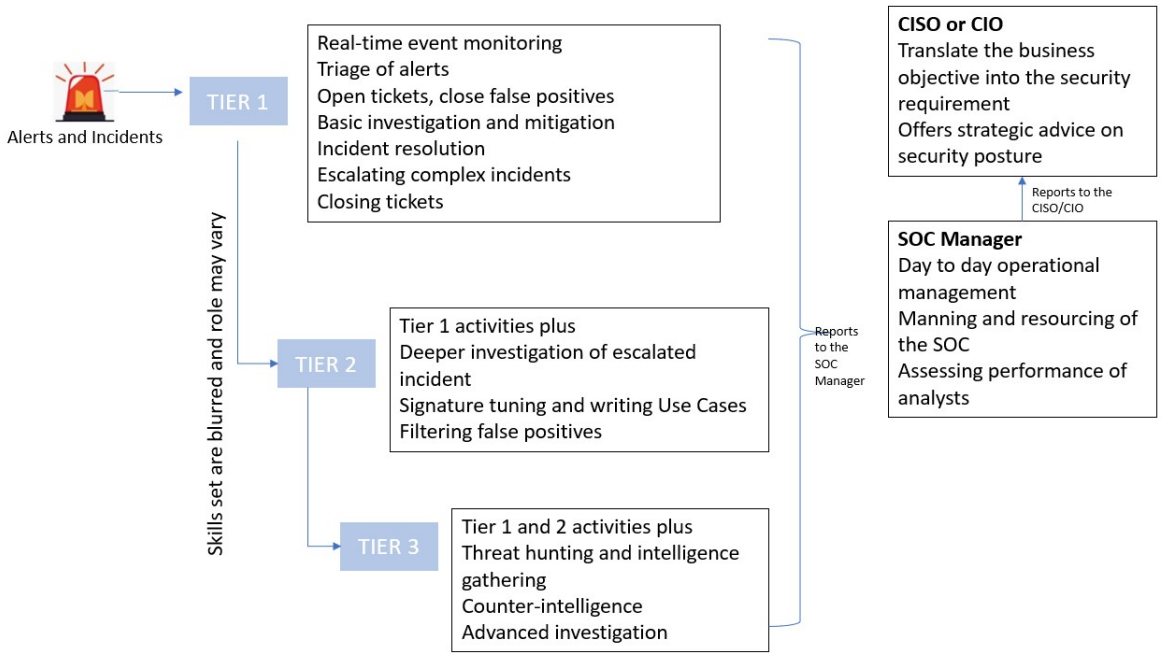

Figure 2.1: Analysts' Tiers and Responsibilities

analyst. Also, according to Kokulu et al. [56], in a non-hierarchical SOC, all analysts are expected to have a similar skill-set.

2.5.4 SOC Manager

Winterborn [9] states that the overall responsibility of a SOC falls to a SOC manager. A SOC manager is responsible for managing the security operations team, providing technical leadership and direction of the SOC in terms of planning future growth [28, 57, 79]. They are directly responsible for managing the individuals and teams within the SOC, including the manning, resourcing and tooling strategy [71, 93]. They run the day-to-day operations of the SOC and report directly to the Chief Information Officer (CIO), or Chief Information Security Officer (CISO), depending on the nature of the organisation. SOC managers are expected to motivate their team, as working in a SOC can be stressful and processes can become mundane [29]. Furthermore, they are responsible for the coordination of communication between stakeholders. SOC

managers are required to gather performance metrics to evaluate SOC performance and must be able to identify and measure key security operations processes. Despite the need to maintain performance metrics, current literature suggests that existing performance metrics used by SOC managers are inadequate and call for further research into this area [25, 53, 56].

2.5.5 CIO or CISO

According to Onwubiko and Ouazzane [38], a SOC, like any other cyber security programme such as IT compliance, needs executive support and their leadership to succeed. This statement is supported by Winterborn [9], who states that without senior/board level support, the SOC will struggle with growth and its objective may not be realised. SOCs need a senior executive's strategic support, as a bottom-up approach to security has a minimal chance of success [21, 100]. According to Schinagl et al. [21], a SOC needs a Chief Information Security Officer (CISO) and Chief Information Officer (CIO) to obtain and justify the SOC's budgetary requirement to the business owners. These two senior executives act as the primary interface between the SOC and the business owner. Although they may not be physically present in the SOC, the CIO or CISO is responsible for translating the business objectives into the security requirements and communicating this to SOC managers [9, 93]. They also offer strategic advice on the security posture of the organisation [53]. The CIO or CISO has a say in the strategies, policies, and procedures used by the SOC to protect the organisation's assets.

2.6 Required Skills for SOC Analysts

The evidence from the literature shows that being an analyst requires curiosity, good analytical skills, and the ability to detect patterns from large volumes of data [54, 57, 93]. Sundaramurthy et al. [25] state that an analyst's skills are dependent on their level of

education and prior experience. SOC analysts must integrate experience and practical knowledge to assess and evaluate observed cyber activity in generating a hypothesis about an event that could indicate a possible attack. According to Andrade and Yoo [53], the cognitive abilities required by analysts include thinking strategies, troubleshooting, inventive thinking, decision-making and learning. They go on to state that to enhance analysts' cognitive abilities, they need hands-on practical training and experience with tools.

Sundaramurthy et al. [25] state that the dynamic nature of cyber attacks and the rapid changes in technology mean that security analysts must periodically undergo training [58]. Incompetent or inexperienced analysts will struggle to deal with complex security incidents and training ensures that analysts have the skills and confidence for their job [25]. Metalidou [101] points out that training is a key factor that increases an analyst's performance. A major challenge faced by most SOCs is recruiting and maintaining the right calibre of analysts [49, 92, 93]. This problem has been further exacerbated by the limited number of cyber security experts with the right skills [102].

Analysts must be able to work under pressure, be curious and abstract thinkers [93]. They must also have a good understanding of some of the most common operating systems, such as Windows and Linux. In addition, they should be able to operate security solutions such as firewalls, IPS, IDS and a SIEM tool [28]. Furthermore, they should possess good problem-solving skills and must have a good understanding of basic computer networking principles [102]. Analysts must be capable of using various technical tools such as Wireshark, Hex Editor, Snort, TCPdump, PDF dissector, and packet analysers [29]. High-performing analysts must have a good understanding of attack techniques, tactics and strategies (TTS) used by attackers, such as the cyber kill chain. Sundaramurthy et al. [25] state that if analysts are not adequately skilled, it affects their confidence when it comes to security incident handling.

The technical skills and qualifications needed to become an analyst can be acquired through formal training courses. For example, in [103, 104], the authors assert that a

bachelor's degree in computer science, computer engineering, or a STEM-related subject is essential for individuals aspiring to become SOC analysts. Naz [103] mentions that individuals without a science background can still become SOC analysts by pursuing industry-specific certifications such as:

Cisco Certified CyberOps Associate: This certification programme is specifically designed to validate the day-to-day tactical knowledge and skills that a SOC analyst needs to detect and respond to cybersecurity threats. This training provides comprehensive knowledge and practical skills related to the duties carried out in a SOC setting [105].

EC-Council Certified SOC Analyst (CSA): This certification provides a concise training programme designed to provide entry-level SOC analysts with valuable skills and knowledge [106].

EC-Council Certified Ethical Hacker: This certification programme provides comprehensive insights into tools employed by hackers, emerging attack vectors, and hands-on training in malware identification and analysis [107].

CompTIA Security+: This certification provides comprehensive training to individuals, equipping them with the necessary skills and knowledge to effectively manage a security incident. It is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career [108].

Certified Information Systems Security Professional (CISSP): This certification is also designed to validate a person's knowledge and experience in the cyber security domain. CISSP holders are expected to have a deep understanding of security concepts and be able to effectively implement them in practical scenarios [109].

Despite the above, research findings indicate a deficiency in individuals possessing the requisite skills necessary for fulfilling cyber security positions [107, 110, 111]. The Department for Science, Innovation & Technology (DSIT) [107] states that a high proportion of UK businesses lack staff with the technical skills, incident response skills and governance skills needed to manage their cyber security. The shortage of skilled

cyber security professionals can be attributed to several factors. For example, firstly, IT security is now a critical component of several industries, resulting in a substantial need for adequately skilled experts. This demand often outpaces the supply of qualified individuals, resulting in many unfilled roles [110]. Furthermore, the field of IT evolves rapidly, with new technologies and frameworks emerging frequently. Staying abreast of these changes necessitates continuous learning and professional growth. Many IT professionals may not have the time or resources to constantly update their skills [112]. Moreover, companies around the world are competing for IT talent, leading to a global marketplace for skilled professionals. This can make it difficult for organisations in certain regions to attract and retain top talent [113]. Also, even when organisations hire skilled IT professionals, retaining them can be a challenge due to competitive offers from other organisations.

In order to mitigate the scarcity of proficient cyber security professionals, including SOC analysts, organisations could adopt various strategies such as allocating resources towards employee training and development, implementing mentorship initiatives to recruit people interested in IT security, providing competitive remuneration and perks, actively pursuing diverse talent, and establishing accessible entry points for individuals seeking to enter the field [114, 115, 116]. Additionally, it is imperative for individuals involved in the field of cyber security to adopt a lifelong learning approach in order to maintain their competitiveness amidst the continuous advancements within this domain [107].

2.7 Challenges Faced By a SOC

SOCs face many challenges, which can impact on their efficiency and effectiveness [6, 36, 45]. Alharbi [43] states that many of the challenges faced by SOCs and analysts can be addressed through research to find practical solutions. However, Kokuku et al. [56] mention that there is little research that seeks to investigate the issues faced

by SOCs and, as a result, the academic community is still unaware of the struggles SOCs face to propose improvement strategies. Chamkar et al. [39] present several challenges faced by SOCs in their work regarding human factor capabilities in a SOC. The challenges faced by SOCs identified in the existing literature are as follows:

- **The Volume of Alerts** - SOC researchers point out that the high volume of alerts generated by monitored devices obscures analysts' ability to identify legitimate threats, which can have a negative impact on a SOC [87, 91, 97]. For example, Feng et al. [42] point out that a single firewall can generate gigabytes of data daily. Likewise, an IPS or IDS can generate thousands of events within the same time period [51, 97]. Yet, the majority of these alerts are false alarms, or false positives [92]. False positives waste analysts' time because they have to investigate them to reach the conclusion of a false alert [56]. Thus, an efficient SOC needs to filter out false positives to reduce the workload on analysts. Kokulu et al. [56] mention that analysts are expected to tune false positives by correcting alerts when they encounter false positives. Sifting through a large volume of data can also result in alert fatigue in the analyst [93].

  The large number of alerts presented to analysts is reported as a contributing factor to analysts' burnout [25]. Analysts are also likely to miss malicious activity because finding what is true becomes like finding a needle in a haystack [42]. According to Tadda [117], correlation systems such as SIEMs can also reduce the number of false alerts. However, he fails to elaborate on why that may be the case.

- **Sophisticated Attacks** - Cybercriminals are increasingly using various sophisticated techniques to avoid detection. The ability to detect stealthy and sophisticated attacks remains a major challenge for many SOCs. For example, Advanced Persistent Threats (APTs) attacks cannot be identified by simply collecting the logs generated by different endpoint devices [92]. SOCs need competent and well-trained analysts to identify patterns in their network that may signal the sign

of a sophisticated attack. However, the level of skills required for detecting lateral movement of APTs is often beyond the abilities of many analysts. With the skills shortage in the cyber industry [9, 17, 118], sophisticated attacks pose a major challenge for inexperienced, or junior analysts [49]. Dealing with sophisticated attacks requires in-depth knowledge and skills on the part of the analysts, which most SOCs do not have [21].

- **Low Visibility into the Monitored Infrastructure** - Kokulu et al. [56] state that one of the major issues facing SOCs today is the lack of complete visibility into an organisation's network infrastructure and monitored devices. Many organisations own a large number of computing devices such as laptops, PCs, routers, switches and firewalls. These devices can grow exponentially, causing SOCs issues with maintaining visibility of the network topology, impeding analysts' ability to maintain effective cyber situational awareness [43, 53, 56]. An outsourced SOC is most likely to face this problem, as they may not have the full picture of the organisation to which the SOC services are offered [74].

- **Regulatory and Compliance Requirements** - Regulatory and industry compliance can mandate a SOC to retain logs over a period of time [119]. Non-compliance to regulatory requirements could lead to regulatory liability, financial penalties and other catastrophic consequences, such as reputational damage, which may have taken years to build [120]. Given that most organisations would not like to risk being fined for non-compliance, there is an onus on the business to provide the SOC with sufficient hardware for log collection. Hardware is expensive, placing an additional financial burden on the SOC. Also, the data collected by SOCs may be subject to privacy regulations.

- **Analyst Burnout** - Information overload and alert fatigue are cited as two of the primary causes of burnout amongst cyber security analysts [25, 65]. Sundaramurthy et al. [25] also report that ineffective performance metrics for assessing the analyst can also lead to frustration, resulting in burnout as they seek to work

towards management metrics that are not reflective of their overall performance in a SOC. Some scholars have investigated and suggested strategies for addressing this challenge. For example, Hull [65] uses a phenomenological interpretive analysis to explore the experiences of SOC analysts as they experience burnout in his doctoral thesis. According to Chamkar et al. [39], automation can be used to reduce analyst fatigue and overall stress as it can be used to perform low-level security actions and assist analysts in handling the number of alerts they receive.

- **Lack of Adequate Performance Metrics for Analysts** - SOC managers use performance metrics to evaluate analysts. Analysts expect objective metrics that consider several aspects of their work. Yet the evidence from the literature suggests that there is currently a lack of a systematic approach for measuring an analyst's performance. The evidence from the literature reveals that current performance metrics are inadequate for several reasons. Chamkar et al. [39] opine that current metrics are inadequate for the following reasons: (1) time-based metrics do not consider the complexity and the severity of the incidents and (2) existing performance metrics do not consider several operational tasks performed by analysts. This study proposes an approach for solving this problem and filling the gap in the current literature. Chapter 4 of this thesis investigates and presents, in greater detail, the need for measuring analysts' performance, the current performance metrics and measures, and the limitations of the current performance assessment methods.

Amongst the challenges presented above, the perception gleaned from the literature is that ineffective performance metrics for analysts negatively affect the morale of analysts, which in turn negatively affects the operational efficiency of the SOC [25]. In [25], the authors described this as a vicious cycle and argued that the lack of adequate metrics to allow analysts to demonstrate their performance effectively also leads to burnout among analysts. While the other challenges are also important, many scholars have called for research on designing effective performance metrics for analysts [49, 53, 54]. This

study therefore focuses on proposing a new method for measuring their performance to address the gap in the literature and the limitations of the current metrics. This research contends that in order to understand the different metrics currently available for assessing an analyst's performance, it is imperative to provide a clear definition of the term "metric" as employed by researchers in the field. Section 2.7.1 presents the definition of the terminology.

2.7.1 Definitions

In the literature, the word metric which is central to this study, is often used interchangeably with other terms such as measures and Key Performance Indicators (KPIs) by both researchers and industry practitioners [55, 121, 122, 123, 124, 125, 126]. However, some researchers in an effort to differentiate these terms provide the following definitions:

A metric - is defined as a quantifiable measure that is used to track and assess performance. A metric is derived from one or more measures [127]. A metric is often used to refer to the measurement of performance.

A measure - is a quantifiable, observable, and objective data supporting a metric [127]. It is a number that can be used in calculations, such as summation, counting, or averaging [127, 128].

A KPI - is a measurable value that demonstrates how well a person or a company achieves key business objectives [129].

Despite the definitions given above, SOC researchers often use the terms metrics, measures and KPIs synonymously when discussing performance assessment methods as reported in [28, 31, 52, 55, 130] and do not pursue a rigorous distinction between these terminologies. A decision was therefore made in this thesis to use these terms interchangeably, adopting a stance similar to that of other SOC researchers in order to identify and consolidate the existing methods for measuring an analyst's performance.

In Chapter 3, the methodology adopted for designing and proposing a new method for assessing the performance of an analyst is presented.

2.8 Chapter Summary - Conclusion

This chapter presented background information on SOCs. The chapter discussed a number of SOC studies that focus on different aspects of a SOC, ranging from models for building SOCs to models for assessing the effectiveness of a SOC, SOC structures, and metrics for assessing analysts' performance. The chapter also discussed the six SOC generations and how SOCs have evolved since its initial inception in the 1970s to give readers an appreciation of how SOC has evolved over time. The different types of SOCs were also discussed, as well as the tier structure used in SOCs, while highlighting that analysts play a vital role in the overall operation of a SOC and that issues affecting them could negatively impact the overall operation of the SOC.

While the challenges faced by SOCs were presented in this chapter, the lack of adequate or effectiveness metrics for analysts, which studies suggest causes low morale among analysts [25], was seen as a major issue causing researchers to call for a solution [49, 53, 54]. Measuring analysts' performance is an important issue because poor performance from analysts impacts the overall performance of a SOC. The next chapter presents the methodology adopted in this study to investigate and propose a novel approach for measuring the performance of an analyst.

Chapter 3

Methodology and Research Approach

3.1 Introduction

This chapter describes the research methodology used in this study to investigate and propose a method for assessing an analyst's performance. The chapter also presents the adopted research methods, the selection of study participants, data analysis techniques and ethical considerations.

As reported in Chapter 2, Section 2.7, one of the main challenges facing SOCs is the lack of adequate performance metrics for analysts. This is a practical problem that requires the use of a practical research methodology [131, 132]. A practical research methodology enables a researcher to design, build and evaluate an artefact in order to solve a research problem [133, 134] as opposed to a formulative and verificational research methodology, which seeks to gain insights and improve the understanding of a problem area [133]. Järvinen [135] posits that the goal of formulative research (also known as exploratory research) is to identify problems for more precise investigation, as well as to gain insights and to increase familiarity with the problem area.

3.2 Adopted Methodology and Justification

Several research strategies were reviewed as shown in Table 3.1 in order to determine the most appropriate approach for the objectives of the study.

Table 3.1: Different Research Strategies [136, 137, 138]

Research Strategy	Main Purpose of the Strategy
Grounded theory	Explain a process, behaviour, event or phenomenon.
Case Study	Understand a case or bring to light a unique case - collecting multiple kinds of data.
Narrative Approach	Gather participants' stories with the aim of restating those narratives.
Ethnography	Explore a phenomenon or an event as it happens in its natural setting.
Transcendental Phenomenological approach	Examine participants' experience and make sense of the experience from a bias-free perspective.
Interpretative phenomenological analysis	Examine participants' thought about a phenomenon experienced.
Hermeneutic phenomenological approach	Examine and interpret documents to capture their underlying meaning.
Phenomenological approach	Examine participants' experience.
Action Research	Focus on solving a problem and examine the impact of the research process on practitioners.
Design Science Research	Focus on designing an artefact for solving practical or organisational problem.

Amongst strategies reviewed, the Design Science Research (DSR) [132, 139] and Action Research (AR) [140, 141] were identified as research strategies that could be used to investigate and address the research problem. These two strategies are well-suited for investigating practical and organisational problems [64, 142]. However, there is a

fundamental difference between DSR and AR, which is mainly around the creation of an artefact [143]. An artefact is a human-made object designed to solve a practical problem [144]. Whereas an AR aims to solve a practical problem through social and organisational change, the DSR seeks to solve a problem by creating an artefact [142, 145]. Johannesson and Perjons [138] explain that while AR does not need the construction of an artefact, they argue that if an artefact is presented as a solution in AR, then it becomes similar to DSR. Similarly, Kumar [64, p.200] states that AR is not a design methodology but a philosophical perspective that seeks the active involvement of research participants.

A major strength to the DSR approach is that it can be combined with other research strategies [138, 146] to explore a research problem in order to create an artefact. In this study, the DSR process is supplemented by the case study methodology to design, build and evaluate an artefact that can be used to evaluate the performance of an analyst. Integrating case studies into the DSR process is similar to the approach presented by Costa et al. [146]. A case study was used during the problem awareness phase as well as the evaluation.

3.3 DSR Process

The DSR process proposed by Vaishnavi et al. [132] is used in this research. According to Vaishnavi et al. [132], the DSR process consists of the following activities:

1. Problem Awareness - Identifying the specific research problem and why a solution is needed. Vaishnavi et al. [132] state that an interesting problem can come from various sources. In this research, the problem was initially identified following a thorough analysis of existing studies on SOCs [49].

2. Suggestion - Vaishnavi et al. [132] state that the researcher must propose a tentative design that can be used to solve the problem. The tentative design is

further developed **through an iterative process** to create new artefacts during the development phase [132]. In this study, a tentative template containing SOC functions and performance metrics developed using insight from existing works [21, 52, 147]. The template was designed using the template analysis technique [148] and shown in Appendix A. The initial objective was to use the output from the template to create a framework that can be used to measure the performance of an analyst.

3. Development - This phase entails creating artefacts for solving the research problem. Table 3.2 shows the different artefacts that can be created in DSR. This study proposes the following artefacts: constructs, a framework, a method, and an instantiation.

Table 3.2: Types of Artefacts [132]

	Output	Description
1	Constructs	The conceptual vocabulary of a domain.
2	Models	Sets of propositions or statements expressing relationships between constructs.
3	Frameworks	Real or conceptual guides to serve as support or guide.
4	Architectures	High level structures of systems.
5	Design Principles	Core principles and concepts to guide design.
6	Methods	Sets of steps used to perform tasks - how-to knowledge.
7	Instantiations	Situated Implementations in certain environments that do or do not operationalise constructs, models, methods and other abstract artefacts; in the latter case such knowledge remains tacit.
8	Design Theories	A prescriptive set of statements on how to do something to achieve a certain objective. A theory usually includes other abstract artefacts such as constructs, models, frameworks, architectures, design principles and methods.

4. Evaluation - This phase involves observing and assessing the effectiveness and efficiency of the artefact. Offermann et al.[131] state evaluation could be achieved through the use of a case study or action research (which demonstrates applicability in practice), expert survey and laboratory experiments or simulations (used to compare different approaches). A number of techniques were applied in this study in order to evaluate the artefacts developed in this research. Amongst them are: member checks, informed argument, logical proof and the Method Adoption Model (MAM). Chapter 7 of this thesis presents the results of the artefact evaluation.

5. Conclusion - Publishing the results. In addition to this thesis, a number of papers were published as part of this study and as a part of peer-review process, received recommendations and suggestions for improving the development of the artefacts. The publications are listed in the introduction chapter under Section 1.5.

Researchers often recommend a cyclical approach to the design process, where the output from each iteration is used as an input for another cycle of a DSR project to either improve the designed artefact or create a new artefact that can also be used to solve the problem. Hevner [149] recommends a three-cycle approach where the output of the first iteration serves as an input for the second iteration of the DSR process. The output from the second iteration also serves as an input for the third iteration. At the end of each iteration, the output must be presented to experts or to the environment where the problem was identified for it to be evaluated. The results from the evaluation determine whether additional iterations are needed in this DSR project [149]. Vaishnavi et al. [132] state that an iterative approach must be adopted in design artefacts until the artefact is adjudged "good enough" for addressing the existing problem by experts or users of the artefact.

The adopted DSR process is shown in Figure 3.1. Although Figure 3.1 appears sequential, the design science project is always executed iteratively, with problem awareness, suggestion, creation, and evaluation occurring in a circular fashion [132, 138].

Following the five step DSR process, the research activities conducted in this study are as follows:

1. Defining the problem through a Systematic Literature Review (SLR). This is presented in Chapter 4.

2. Making initial suggestions on how existing SOC frameworks can be used as the basis for addressing the identified problem. This is presented in Chapter 5.

3. Conducting interviews with SOC experts to deepen understanding of the problem and improving the initial templates. This is presented in Chapter 6.

4. Development of the following artefacts: 1) constructs, 2) a SOC conceptual framework, 3) the SOC-AAF and the 4) SOC-AAM using an iterative approach. This is presented in Chapter 6.

5. Evaluating the proposed artefacts. This is presented in Chapter 7.

6. Publish the results as a dissertation and other scholarly articles as discussed in the introduction chapter under Section 1.5.

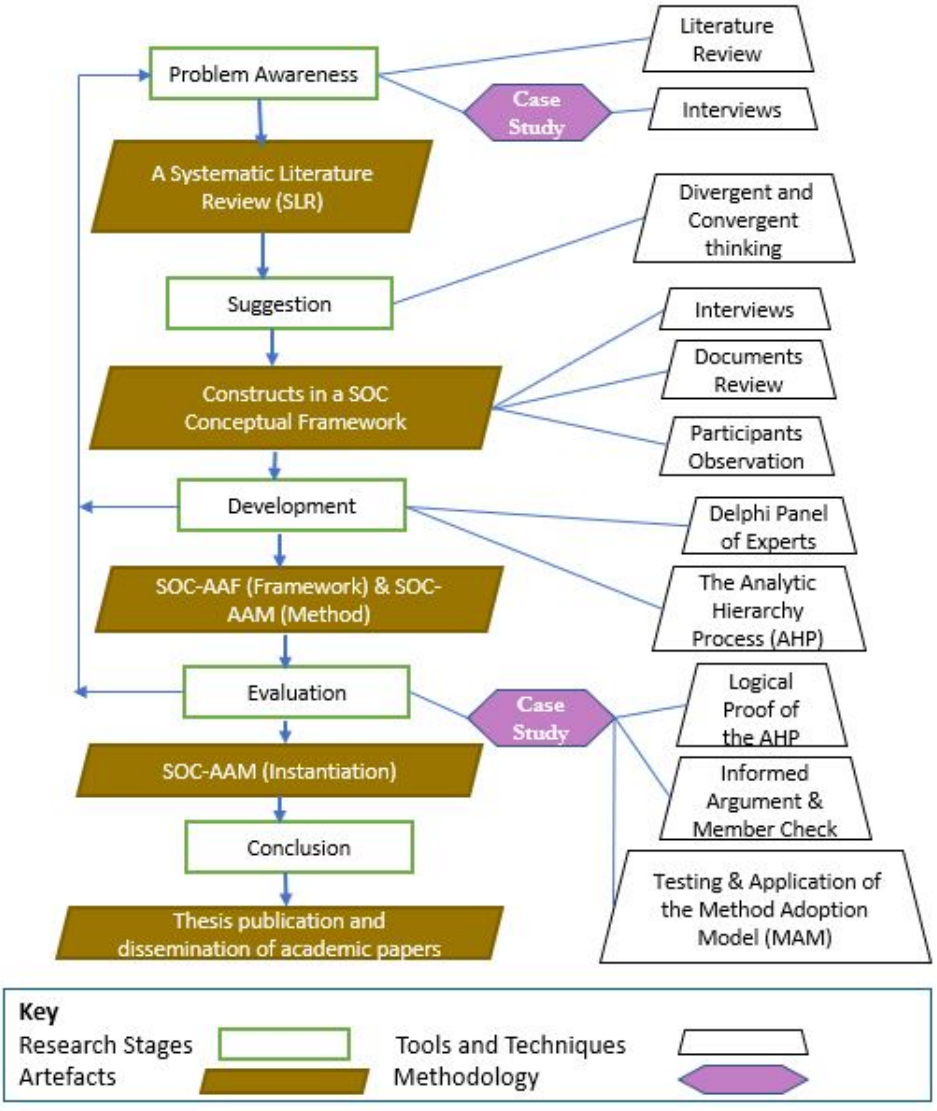

Figure 3.1: DSR Process [132]

3.3.1 Integrating a Case Study into the DSR Process

Yin's [150] approach to case study design (Figure 3.2) was exploited in this research and integrated into the DSR. Yin's case study methodology provided the framework for defining the research questions, designing the interview questions, obtaining ethical approval for the study, recruiting participants for the study, and evaluating the proposed artefacts. It is important to highlight that the phases shown in Figure 3.2 are conducted in a linear but iterative manner so a researcher can move back and forth between the phases during the research project [150]. The linear process is as follows: planning, designing, preparing, collecting, analysing, and sharing. However, Yin [150] acknowledges that each step requires the researcher to review and reexamine the previous decision, resulting in a linear but an iterative approach.

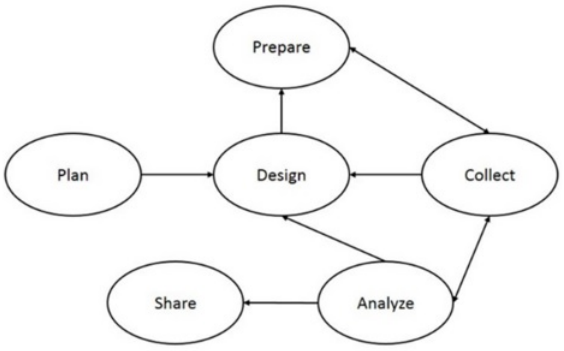

Figure 3.2: Case Study Research Process [150]

The 'plan phase' of this research involved developing and establishing the research questions. It also involved conducting a literature review to gain a better understanding of the problem. During the 'design phase,' the interview questions in Appendix B and a preliminary template - (Table 1 - Appendix B) containing the functions of a SOC were created. As part of the 'preparation phase', ethical approval was sought from the University's Research Ethics Committee (Approval ID: COMSC/Ethics/2019/063) before embarking on any empirical data collection. As in any other kind of research, design science researchers need to address ethical issues [138]. The goal of the ethical approval was to safeguard participants' interests and ensure that their participation in

this study was voluntary and based on informed consent.

The interview questions were developed using insight from existing works and are grounded on the functions of a SOC as suggested by previous researchers [21, 25, 30, 52, 54]. These functions are discussed in Chapter 5. The questions were then reviewed by the research supervisory team in order to ensure that they captured the information needed to answer the research question before contacting and recruiting the participants for this study. The draft interview questions were also piloted using a SOC manager and analysts at a SOC that supported this study to check the clarity of the questions and to ensure that the study participants would understand the questions.

The 'collection phase' entailed collecting empirical data from SOC experts. The data collection methods used in this research are discussed under section 3.4.

The data collected from the study participants was analysed ('analysis phase') using the techniques discussed in section 3.6. The 'share' phase entailed the publication and dissemination of research papers and this thesis.

3.4 Data Collection Methods

In order to address the research problem, a number of research methods were used as a part of the DSR process. The selected research methods were influenced by the issues the researcher wanted to investigate. In line with the research aim and objectives, the researcher wanted to understand, from the perspective of SOC experts, metrics for assessing the performance of an analyst and how to improve the assessment method. The researcher also wanted to engage directly with SOC experts to get a deeper understanding of analyst functions and metrics. The researcher also wanted to work closely with industry practitioners to build and evaluate a new method for assessing the performance of an analyst.

Additionally, the selected methods were influenced by the practicality and availability

of resources, in particular, time constraints and access to data sources and participants. Interviews, participant observations, document analysis [137], the Analytic Hierarchy Process (AHP) [68], the Delphi method [151], and surveys [64, 152] were considered relevant methods that could be used to investigate and address the research questions.

A comprehensive rationale and justification for the utilisation of each method are outlined below.

3.4.1 Interviews

A one-to-one semi-structured interview [55, 153] was used to solicit SOC experts' opinions on existing performance metrics and measures for analysts. A semi-structured interview allows the researcher to ask the interviewee pre-determined questions but with the flexibility to probe participants with additional questions that were not planned in advance. The interviews were used to understand the role of analysts, metrics for assessing their performance and how analysts' assessment methods could be improved to capture their performance. Interviews allow participants to describe what is important to them [154]. The interview data is stored in the following location:

https://git.cardiff.ac.uk/c1854157/interviews-transcripts.git

However, this research acknowledges that interviews have some drawbacks. Firstly, conducting interviews and analysing the interview data is a time-consuming method because it requires bringing together statements from different participants and it is usually difficult to make links between the varied perspectives [154, 155].

Secondly, interviews are also susceptible to bias as interviewees may want to please the researcher and, as a result, provide answers they believe the researcher wants to hear [154]. Doody and Noonan [154] suggest that the desire of participants to create a good impression may lead to participants not answering honestly. To minimise this drawback, researchers often interview multiple participants to identify common themes rather than relying solely on a single person [156]. Participants can also be interviewed until the

point of saturation, where new themes stop emerging from the interview data [56]. This is an important validation technique in qualitative research [56].

Despite their limitations, interviews have been used by many studies that focus on SOCs [29, 79, 80]. For example, Hámornik and Krasznay [79] conducted a semi-structured interview with SOC experts to investigate incident handling processes, roles, and tools used in a SOC. Similarly, Schinagl et al. [21] also utilised interviews to engage with SOC experts to design a framework for measuring the performance of a SOC. Goodall et al. [51] also conducted interviews with analysts to gain an insight into the work of intrusion detection analysts. The demographic information of the interview participants is presented in Chapter 6.

3.4.2 Participants Observation

As a part of this study, SOCs were visited to conduct the face to face interviews with the SOC experts. Visiting SOCs provided an opportunity to observe SOC managers and analysts at work in their natural environment.

From the researcher's perspective, having an understanding of analysts' work processes and functions was useful in assessing how performance could be measured.

Despite the benefits of observation, some researchers assert that participants can change their behaviour when they know that they are being observed [157]. The work processes and functions observed such as monitoring of security alerts on a variety of consoles and analysing incidents corroborated with the findings in the literature [52].

3.4.3 Documents Analysis

The research also includes document analysis. The document analysis refers to the examination of materials containing information about the subject of the study [158, 159]. The documents reviewed as a part of this study are analysts' handover notes and

SOC work instructions. The goal of the document analysis method [159] was to gain a deeper understanding of the operation of a SOC as well as the role of an analyst. This review enables the researcher to gather data to corroborate with data gathered through other methods.

The document reviews also provided insight into the types of incidents typically handled by analysts and the priorities assigned to these incidents. This data supplemented what had been previously identified in the literature and through the interviews to confirm the initial theme developed from the existing literature.

3.4.4 Analytic Hierarchy Process (AHP) Method

To achieve the aim of this research, this study introduced the AHP into a SOC in order to design a new formal approach (the SOC-AAM) for measuring the performance of an analyst. The AHP was used in this study to propose a weighted approach for measuring analysts' performance accounting for the level of importance of an analyst's function.

The AHP was found to offer a practical framework that can facilitate the collection of data from SOC experts in order to design a new approach for measuring analysts' performance.

The AHP can be used to compare objective and subjective criteria and make a judgement on their relative importance in order to derive weights for the criteria [68]. The AHP allows for the inclusion of quantifiable and intangible criteria. To the best of the researcher's knowledge, this is the first study to introduce the AHP into a SOC setting and specifically, as the basis for measuring the performance of analysts working in a SOC.

Some applications of the AHP in the fields of information systems and computer science are summarised below. Ghanbari and Othman [160] drew on the AHP to propose a priority-based job scheduling algorithm for cloud computing. Benìtez et al. [161] drew on the principles of the AHP to develop an algorithm, which they integrated into

a decision-making network for a water management system. Similarly, Bradie and Lashkari [162] utilised the AHP to establish the relationship between the lack of security awareness and computer security risk and the ranking of the risk. Fahmy [163] used the AHP to ascertain how the reliability of a distributed system can be controlled by assigning weights to its components. The work by Bodin and Epstein [164] proposed a model to rank the players of an existing baseball team in preparation for the expansion draft. Bodin and Loeb [165] used the AHP methodology to assist Chief Information Security Officers in optimising the allocation of a budget for maintaining and enhancing the security of an organisation.

The AHP requires that the evaluation criteria and subcriteria be clearly defined and require the input of experts [166, 167]; thus there is a need to engage with SOC experts. Chapter 6 provides a detailed description of the constructed artefacts through case studies with SOC experts.

The AHP is founded on three fundamental principles: (1) decomposition - by dividing a complex problem into modular components and organising these components into a hierarchy; (2) comparative judgements - by assigning numerical values to the criteria/elements in the hierarchy based on pairwise comparisons of the relative importance of each of the criteria; and (3) synthesis of priorities - by combining the judgments to obtain the criteria weights [68, 168].

After determining the criteria weights, a consistency check is performed to confirm that the judgement was not made arbitrarily [68]. The objective of the consistency check is to reduce bias in the pairwise comparison process. If judgements are found to be consistent, then the proposed weights can be used as the basis for the decision. On the other hand, if the judgements are inconsistent, Saaty [68] recommends re-evaluating the judgement. The application of the AHP is presented in Chapter 6.

3.4.5 Delphi Method

The Delphi method was integrated into the AHP in order to solicit the opinions of SOC experts during the data collection phase in order to develop a new method for evaluating analyst performance. Developed by the RAND Corporation in the 1950s, the Delphi method is a strategy for achieving a consensus judgement from a group of experts or knowledgeable participants [169]. The Delphi method is a particularly useful method to employ in situations where there are no standard evaluation criteria [20]. It offers a controlled way of collecting data from experts through a series of rounds.

However, the Delphi method has some shortcomings. For example, it can be a laborious and time-consuming method due to the number of rounds and associated feedback provided to participants for each round.

There are several variations of the Delphi method in the literature, giving researchers options depending on what they want to investigate [170]. In this research, the decision-making Delphi technique is used as it follows a structured approach that allows a group of experts to create a future reality based on the choices that they make [69, 170]. According to Arof [170], the decision-making Delphi method is very similar to the classical Delphi technique because they follow similar steps. These steps are summarised in [171] as follows: (1) design the questionnaire and select the Delphi panel; (2) conduct the first round of the Delphi exercise using the expert panel; (3) synthesise the opinion provided by the experts from the first round and provide that feedback to all the members of the panel; (4) request that each member of the panel reconsider the decision based on the findings from the experts from the first round; (5) synthesise expert opinion from the second round and reach a consensus; (6) repeat steps 3 to 4 (if necessary) until a uniform result is achieved on the topic. This six-step approach was followed in conducting the Delphi exercise.

The application of the Delphi method as a part of the AHP in what this study refers to as the Delphi-AHP exercise [170, 172] is presented in Chapter 6.

3.4.6 Survey

The final data collection method used in this study is a survey. The survey design and application is presented in Chapter 7 under Section 7.3.3.2. The purpose of the survey was to get feedback from the SOC experts on the SOC-AAM. The survey contained a series of Likert-scale questions based on the Method Adoption Model (MAM) which is described in detail in 7 under Section 7.3.3.2. The Likert-scale provided a closed set of questions which the participants had to response to in order to fit into pre-defined categories as follows: strongly agree/agree/neutral/disagree/strongly disagree. Additionally, the survey included on the form some open questions to allow the SOC experts to express their opinion on what they thought about the SOC-AAM in their own words.

A survey as reported in the literature offers a cheap, quick and efficient way of gathering data from a group of people [64]. It is cheap and quick because the researchers do not have to be present when completing the survey; hence saving on travelling costs and time.

3.5 Selection of Study Participants

Researchers cite a number of techniques for selecting participants for a study [64, 137, 157]. However, two of the most popular techniques are probability sample and 'non-probability sample' (also known as purposive sample) [137, 155]. A probability sample offers a researcher a true image of the entire population, as members within the research population have an identifiable chance of being selected. Under a probability sample, all the people within the study population have an equal chance of being selected to participate in the study.

On the other hand, a purposive sample involves explicitly selecting participants because the researcher believes that they have the relevant experience and/or unique insight

about the issues understudy, for example, through their professional role.

In this study, SOC analysts and SOC managers were 'purposively' [173, 174] selected because they have direct experience on the topic. The chosen analysts and managers participated in a one-to-one interview, a Delphi exercise, and an experimental case study to evaluate the SOC-AAM.

3.6 Data Analysis Technique

Braun and Clarke [175] state that if one does not know how a researcher analysed their data, it would be difficult to comprehend how they arrived at their conclusions or the assumptions that informed their analysis and subsequently their findings. They further argue that evaluating the work of those who do not clearly state the techniques they used to analyse their data and how they can be compared to others on the same topic will be difficult. With this in mind, a detailed description of the data analysis technique employed in this study is provided.

Rose et al. [155] state the data collected by a researcher has an implication on the analysis technique that can be used. However, Green and Thorogood [176] opine that most researchers usually use a combination of approaches to analyse their data. Since this study draws on a range of research methods, various data analysis techniques were utilised. A number of data analysis techniques were applied to the different data collected in this study, as discussed below.

3.6.1 Analysing the Qualitative Data

To analyse the interview data and the documents reviewed, the thematic analysis technique was utilised. The thematic analysis method is a well-known data analysis technique for identifying, analysing, and reporting themes or patterns in data [175]. A theme is described as anything important about the collected data that facilitates the

understanding or answering of the research question [177]. A theme represents some level of patterned response or insight observed within a collected data set [175]. The themes in this study are the functions of a SOC, the functions of an analyst and metrics for measuring an analyst's performance.

It is important to highlight that the thematic analysis technique is a broad category of methods for qualitative data analysis that seeks to uncover themes within the data set [178] and as such there are various versions of the thematic analysis method. In this research, a version of the thematic analysis method referred to as the 'Template Analysis' (TA), was used. The TA was developed by King [148] for analysing qualitative data. The TA was selected because it allows researchers to define *a priori* themes [178] before engaging with the study data, unlike other versions of the thematic analysis, such as the one proposed by Braun and Clarke or Framework Analysis [175]. In using the TA technique, an inspiration is drawn from Sundaramurthy et al. [179] who used a similar data analysis technique in their work on SOCs.

Analysing data using the TA technique entails the creation of a coding 'template' that summarises and organises the themes identified as significant in a data collection by the researcher(s) [159]. Once *priori themes* have been defined, the first step in the analysis is to read through the qualitative data, making a note of any segments that appear to tell the researcher something relevant to the research questions. Such segments are coded as such when they correspond to a priori themes. Otherwise, new themes are defined and organised into an initial template to include the relevant material.

Using the information from Appendix A which details the initial set of themes, Table 1 in Appendix B was devised and used during the interviews. The themes were developed based on the information the researcher is interested in identifying from the data. The initial themes are based on a SOC's functions and the metrics reported in the literature for measuring performance under the function. These themes were defined using insight from existing academic literature and the insight from the SOC documents reviewed during SOC visits. These themes were subsequently refined following the interviews

with the SOC experts to create the template in Appendix C. The template in Appendix C shows the functions of a SOC, the functions of analysts and metrics for measuring the performance of an analyst under each function (See Table 2 in Appendix C). The template also includes indicators that can be used to assess the quality of incident analysis and report, based on the input from SOC experts who participated in this study. Chapter 6 presents a discussion on the analysis and the findings.

3.6.2 Analysing the Quantitative Data

The data collected using the AHP method along with the Delphi process was analysed using a well-defined process offered by the AHP framework. The AHP provides a mechanism for checking the consistency in the decision matrices or the judgements made by the study participants to ensure that the decisions are sound and not made arbitrarily [68]. Section 6.5.3 Chapter 6 presents the results of the analysis.

The survey data collected was analysed using statistical testing and discussed in Chapter 7 under Section 7.3.4.

3.7 Validity and Reliability of the Study

The study's validity and reliability were assessed quantitatively as well as qualitatively. The quantitative portion of the study was based on hypothesis testing. The survey instrument was tested for validity and reliability using the Cronbach's alpha. This is presented in Chapter 7 under Section 7.3.4.

From a qualitative research perspective, the validity and reliability of the study were evaluated in terms of (i) credibility, (ii) transferability, (iii) dependability and (iv) confirmability. These four areas are usually used to assess the validity and reliability of a qualitative study [64, 66, 155, 180, 181].

Credibility - Sullivan and Sargeant [66] state that the credibility of a research starts with a robust review of the existing work. This study began with a thorough analysis of the existing work through a SLR. Creswell and Creswell [182] also assert that the credibility of qualitative research involves evaluating the collected research data to ascertain whether it is believable from the participants' points of view. Unlike quantitative research, a qualitative researcher is not seeking for a single truth but rather to understand multiple realities. Creswell and Creswell [182] explain that both the researcher and the participant of the study determine the credibility of the study through accurate reporting of the findings from the viewpoint of the participant and the researcher. In this research, it is the SOC experts that can judge the credibility of the outcome of the study since they shared their experiences on how they think an analyst's performance needs to be measured.

Qualitative member checks and triangulation were applied to establish the credibility of this study. Multiple sources of evidence are used to achieve triangulation, including interviews with multiple study participants from various industries, observations, documents reviews as well as a thorough analysis of the existing works on SOCs. The member check technique, which involves checking with the study participants whether the researcher's interpretation of their opinion is accurate, was also used to improve the credibility of this study.

Dependability - Rose et al.[155] posits that the dependability of a research is about demonstrating that the findings from the study are consistent and that it could be repeated. Sullivan and Sargeant [66] state that dependability and reliability are interlinked. They opine that a technique for ensuring dependability and reliability is the use of triangulation, in which multiple sources of data are used. Another technique for ensuring the reliability of the data is to collect data until new themes stop emerging, a process known as saturation point. Interview data from participants was collected until the point of saturation.

Transferability - Transferability relates to the extent to which the outcome of the study

can be transferred to another context. The transferability of a qualitative research, according to Kumar [64] rests on the researcher as it involves providing enough information to allow others to assess the relevance of the findings in other contexts. Transferability is associated with external validity and applicability [64]. To facilitate transferability, a detailed description of the setting in which the study took place is presented. Participants' demographic information is also presented in Chapter 6 to allow readers to understand the experience level of the participants as well as the industry within which they operate.

Confirmability - The confirmability of a study, also known as objectivity, denotes the extent to which the study's findings are confirmed by others [64]. Confirmability involves demonstrating that the findings are shaped by the participants and not by the opinions or the biases of the researcher [155]. In this study, several analysts and SOC managers were engaged to allow the findings from different participants to be confirmed by other participants. The information was recorded to avoid misinterpretation of the interview data. The re-checking of the interview data through member checks was used for confirmability of the output. Member checking also helps a researcher reconfirm and clarify any further queries resulting from engaging with study participants [183, 184].

3.8 Ethical Considerations

This study was carried out in strict adherence to the research ethics policy of Cardiff University. Ethical approval was sought from the Cardiff University research ethics committee before embarking on this research (Approval ID: COMSC/Ethics/2019/063 - See Appendix N). Participants were asked to sign an informed consent form to approve their participation in this work (See Appendices O, P and Q). To ensure transparency, the consent form clearly explains the nature of this study to the participants, the study's objectives, and the rights of the study participants. Participants expressing interest in the

study were also made aware that their participation was voluntary and had the choice to withdraw from the study at any time during the research.

The participants' identities and the organisations that participated in this research were all anonymised. To preserve privacy and confidentiality, individual analysts' opinions will not be disclosed to one another. Every effort was made to ensure that the study did not raise any ethical concerns for the participants or involved organisations.

3.9 Chapter Summary - Conclusion

This chapter presented the methodological approach adopted for this research. The chapter discussed the research methods, the selection of study participants, data analysis techniques and ethical consideration issues informing this research. The DSR is used as the main research design and is complemented by the case study methodology [150]. The next chapter presents the first phase of the adopted DSR process. It also presents a comprehensive investigation of the problem domain with the aim of formulating a solution to the problem.

Chapter 4

Exploring Performance Metrics for SOC Analysts

4.1 Introduction

This chapter presents a thorough examination of the problem domain. The chapter investigates current performance metrics and explores the problems with the existing metrics. The chapter begins with a discussion regarding the need for measuring performance in a SOC and highlights the importance of performance measurement in a SOC.

4.2 Importance and Purpose of Performance Measurement

Researchers have discussed and documented the importance of performance measuring. Fekete and Rozenberg [185] state that the long-term survival and competitiveness of an organisation rests on its ability to measure the performance of the employees and to scrutinise their contributions in achieving the objectives assigned to them by managers. According to Gunasekaran et al. [186], individuals working within an organisation must be held accountable for their individual work performance. Individual work

performance denotes how much an employee contributes to the overall organisational goal [187].

Islam and bin Mohd Rasad [60] state that if an employee does a good job, they would expect this to be recognised by management through a performance assessment process. They also argue that if there is no assessment, poor performers will believe that their level of performance is acceptable. Taj and Kumaravel [188] assert that an employee measurement system enables the evaluation and reward of employees. Brotby and Hinson [189] opine that where there is no performance evaluation, employees may assume that their performance is adequate regardless of how they are performing.

Analysts working in a SOC are expected to demonstrate a high level of operational performance because poor performance could negatively impact the overall effectiveness and efficiency of the SOC [10, 42, 190]. Given that analysts in many SOCs are expected to work independently on problems [57], measuring analysts' performance would allow those performing well to be acknowledged and rewarded [25, 54, 188]. Fekete and Rozenberg [185] state that a performance measurement tool could be used to communicate performance expectations to employees and provide them with feedback.

Onwubiko [52] opines that SOC managers could use performance metrics to motivate analysts to improve their performance but he fails to elaborate on how the assessment could be used as a way of motivating analysts. Sundaramurthy et al. [25] mention that SOC managers could use performance metrics to determine how well an individual analyst is performing within the team and to check that analysts are getting the job done [25, 52]. According to Sundaramurthy et al. [25], a top-performing analyst can expect promotions and other perks associated with contributing to the team's goals. Measuring performance could provide opportunities for recognition and identify areas where they need to improve. The outcome from any performance evaluation could be used to identify training needs for an analyst [127].

Despite the advantages of using performance metrics, the perception gleaned from the literature is that current performance measurement methods for analysts are problematic

and do little to motivate them. This is because researchers suggest that the existing metrics do not capture the full spectrum of the work expected of an analyst [25, 54, 179]. Sundaramurthy et al. [25] state that the lack of an adequate and a systematic approach for evaluating an analyst's performance leads to low morale, a decrease in analysts' productivity, and lessens their enthusiasm. This is because analysts are unable to fully demonstrate to their managers their range of work during performance assessment. According to Sundaramurthy et al. [25], the more reflective an analyst's performance is to the performance metrics used, the greater their confidence during their evaluation. A performance measurement system that is well designed and properly used is vital for the effective functioning of an organisation [59]. It is, therefore, an objective of this study to propose an approach for measuring the performance of an analyst taking into account the diverse work they undertake using the DSR process.

The first step of the DSR process applied in this study as discussed in Chapter 3 (section 3.3) is to use a SLR to investigate the existing performance metrics and to identify the problems associated with them. The section below presents the SLR.

4.3 Literature Review Methodology

A SLR was conducted to identify relevant articles on SOCs to facilitate the understanding of performance metrics for analysts and their limitations. The literature search also sought to identify any SOC framework and/or model for measuring an analyst's performance.

The review process was driven by the guidelines for conducting SLR suggested in [191]. A SLR is a type of review that collects multiple research studies and summarises them to answer a research question using rigorous methods [191, 192, 193]. The literature review is expected to answer the following questions:

- *(RQ1) What metrics exist for measuring analysts' performance in a SOC? What*

are the strengths and limitations of existing metrics?

- *(RQ2) What frameworks and/or models exist for measuring the performance of an analyst? Is there a comprehensive framework, model or method for measuring performance?*

In order to answer the above research questions, articles were selected from the following five major academic databases: Scopus, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Association of Computing Machinery (ACM) Digital Library, Springer and Elsevier ScienceDirect. These databases were specifically selected because they are rated amongst the top scientific databases for computer science and cyber security research and cover many of the top conferences and publications [20, 177, 194]. The selected databases were complemented with searches on le and Google Scholar to ensure that no important publications (grey literature) were overlooked, as the topic of SOC is also driven by industry [57]. Moreover, Rose et al. [155] mention that Google and Google Scholar offer researchers the ability to search across many academic and other scholarly articles.

The keywords used for the selection of papers were “security operations centre”, “security operations center”, “security operation center”, “security analyst”, “metrics”, “performance metric”, “performance metrics” “framework”. The term ”SOC” is not used to search for papers since it also represents an abbreviation to other terms such as System on a Chip (SoC), resulting in a significant number of false positives. Table 4.1 presents a summary of the literature review protocol and strategy.

The following criteria were used to select papers for review:

- Papers that have been published in peer-reviewed academic journals, workshops, or conference proceedings. Knight and Nurse [177] explain that selecting peer-reviewed articles increases the likelihood of finding and including high-quality and objective contributions. This is because, in most cases, such papers have been independently evaluated by subject matter experts.

- White papers and reports from reputable organisations well-known within the cyber industry, such as the SysAdmin, Audit, Networking, and Security (SANS) Institute, and the National Institute of Science and Technology (NIST), as their contents would have been independently evaluated by subject matter experts in the field before their publication.

- The search was restricted to literature written in English. No restrictions were placed on year of publication, as a SOC is a relatively new field, and placing year restrictions could eliminate important research papers.

- The reference lists of selected papers were also reviewed for additional studies relevant to this research.

Table 4.1: Review Protocol

Search Date	Search Engine Start Date - December 29th 2021
Databases	Scopus, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Association of Computing Machinery (ACM) Digital Library, Springer and Elsevier ScienceDirect
Search criteria	English; Search Keywords in Title, Abstract and Keywords
Search keywords	(“security operations centre” OR “security operations center” OR “security operation center” OR “security analyst”) AND (“metrics” OR “performance metrics” OR “performance metric” OR “framework”)
Search methods	Keyword search and snowballing.
Inclusion criteria	Addresses SOC in general or part of it. Journal or Conference Paper. Full text of paper available.

In line with the generally accepted SLR process proposed in [191], the title and abstract of each paper returned by the databases were read to determine the article’s relevance to

this study. Reviewing the abstracts and titles constituted the first step of the literature search process. The studies that discussed SOC operations, SOC metrics and performance metrics were included. The articles that did not have sufficient information on the subject in the abstract were excluded during stage one. Next, the introduction and conclusion of papers deemed relevant to this study were reviewed. This step constituted stage two of the search process. The final step in the review process was to read in full papers whose introduction and conclusion were deemed pertinent to this research. The sections below provide answers to the research questions posed.

4.4 Performance Metrics: Strengths and Limitations

This section addresses research question 1 (RQ1): *"What metrics exist for measuring analysts' performance in a SOC? What are the strengths and limitations of these metrics?"*

A review of the literature reveals that a number of performance metrics (also referred to as KPIs by some authors) [28, 31, 129] exist for measuring the performance of an analyst. Sundaramurthy et al. [54] report that some SOCs count the number of incidents raised by an analyst as a metric to measure their performance and that counting the number of incidents raised at the end of an analyst shift is used by some SOCs to determine how well the analyst performed. However, in [179] the authors report that, by using such a metric, some analysts may choose to raise a large number of benign or low-priority events in order to impress their managers in comparison to their peers who are dealing with critical, more challenging and time-consuming incidents [179]. The authors also report that some SOCs focus on the time it takes an analyst to investigate a security incident to assess their performance. However, researchers have commented that a limitation to time based metrics such as the time it takes an analyst to investigate an event fails to take into account the complexity of the incident and, as a result, does not present a clear picture of an analyst's performance [56].

Sundaramuthy et al. [25] report that some SOCs measure analysts' performance using the time it takes them to create a security incident ticket. However, they point out that analysts are dissatisfied with time-based metrics because some incidents naturally take longer than others due to their complex nature. They also report that analysts bemoan that several aspects of their tasks, such as dealing with false positives and tuning them out, are often not recognised in the evaluation process [39]. This is disappointing because researchers such as Onwubiko [52] highlight that reducing false positives is an important activity, as it reduces the volume of alerts presented to an analyst. Interestingly, Sundaramuthy et al. [25] found that SOC managers do not know what to measure and find it challenging to devise a useful approach to measure analysts' performance. They argue for research that defines a meaningful approach that could be used to assess analysts' performance.

Sundaramurthy et al. [58] state that an analyst's performance in a SOC could be based on the number of incidents detected at the end of a given day. However, they caution that using such a metric could result in analysts spending less time on an incident to investigate it in greater detail, as their performance is based on the number of closed incidents rather than the time spent on it. This problem can be resolved if SOC managers also assess performance based on the incident analysis performed by an analyst [35].

Schinagl et al. [21] proposed an assessment method for SOCs that includes measuring analysts' competencies and experience. They evaluate competence and experience using a 5-point Likert scale questionnaire (1= unsatisfactory, 2= concerned, 3= suboptimal, 4= satisfactory, 5= desired). The questionnaire is centred around the various aspects of SOC operations and the experience of analysts. Their assessment output is a spider diagram generated following an in-depth discussion with analysts working in different SOCs. Even though the Dutch security community has accepted their model as a model for building and improving SOC services, specific analysts' tasks or functions measured were not explicitly defined in their paper. Also, the authors do not elaborate on how their ratings were synthesised to achieve the analysts' overall performance. Furthermore, it

is unclear whether the most significant aspects of analysts' functions are captured in their work as part of their evaluation. Another drawback with their approach is that their assessment method, in the form of a questionnaire, was based on analysts' intuition, and the result is, therefore, likely to differ from one evaluator to another [195, 196]. Also, another issue with using a self-assessment questionnaire is that people may be inclined to judge their own performance favourably [197]. As a part of this study, the researchers were contacted to request further information on the aspects of analysts' operations that were measured. Unfortunately, the researchers did not provide this information, suggesting that the project had ended and the data was no longer available.

Despite the downside to using a self-evaluated questionnaire as a method for evaluating performance discussed above, McClain [102] also uses a questionnaire based on a 6-point scale to measure the experience of analysts on eight (8) cyber security software tools. McClain et al. [102] state that analysts reporting a higher level of experience using these tools outperformed their less experienced counterparts in a training exercise.

Onwubiko [52] presents a number of metrics that could be used to evaluate analysts' performance. The metrics include the number of incidents detected by a SOC analyst in a certain period, the number of false positives, and the time taken to raise incidents. However, as pointed out by Sundaramurthy et al. [29], there are drawbacks to using the number of incidents raised and the time it takes to raise an incident as a performance indicator. Furthermore, these metrics do not provide a complete view of an analyst's performance, as they may perform different functions in the SOC [25, 54]. It is important to highlight that these performance metrics are used as standalone and do not allow an analyst's overall performance to be captured.

Shah et al. [35, 87] propose measuring analysts' performance based on the number of alerts processed by a sensor assigned to an analyst for real-time monitoring. According to Shah et al.[35, 87], in a SOC where analysts are allocated to specific sensors, analysts' performance could be assessed based on the number of analysed or unanalysed incidents at the end of the shift, taking into consideration the volume of traffic sent to that sensor.

Their approach uses a metric known as the average total time for alert investigation ($avgTTA$). TTA represents the sum of the waiting time in a queue and an analyst's investigation time of an alert once it arrives in their database. They assume that a SOC will employ analysts of the same capability in order to compare the effort of analysts. Unfortunately, most SOCs will not be in a position to employ analysts with the same capability [29]. Another limitation associated with their approach is that their assessment method can only be used by SOCs using sensors such as IDS or an IPS. In practice, however, studies suggest that analysts perform many tasks other than the monitoring and analysis of alerts [46, 56].

Shah et al. [91] suggest a number of criteria that can be considered when devising generic performance measures for a SOC. They identify false positive, false negative, true negative and true positive decisions made by an analyst when investigating an alert as essential factors. Shah et al. [91] also discussed the average time it takes for an analyst to respond to an alert presented to them as an approach for assessing their performance.

The study by Kokulu et al. [56], which focuses on issues faced by SOCs, identified performance metrics such as the number of incidents raised by an analyst and the time it takes an analyst to respond to an incident as ineffective because it does not take into consideration the severity of the incidents to differentiate the efforts of analysts on the basis of the priority of the incidents they handle. Onwubiko and Ouazzane [72] point out that cyber security incidents are classified in terms of severity or priority. Kokulu et al. [56] also point out that the use of time taken to respond to an incident as a measure causes controversy between analysts and SOC managers, but they fail to elaborate on this critical point. Kaur and Lashkari [86] also present performance metrics such as the time taken by an analyst to create and resolve tickets, the number of tickets raised by analysts, the quality of incident report, the number of incidents, number of alerts analysed or unanalysed, and average time taken to raise or detect the incident, as some of the metrics typically used by SOCs.

Chamkar et al. [39] also present a number of metrics that SOC managers can use to measure the performance of an analyst. Among the metrics suggested by Chamkar et al. are: the average time to detect a security incident; the average time to respond including applying the technical countermeasures and closing the case; the number of processed and analysed alerts during the analyst's shift and the number of resolved security issues or closed tickets by shift. These metrics are similar to those reported by scholars such as Kokulu et al. [56] and Onwubiko [52].

Onwubiko and Ouazzane [72] discuss several time-based performance metrics used by SOCs that can be used to evaluate analysts' performance. Amongst the time-based metrics is the Mean Time To Detect an incident (MTTD) - also known as Mean Time To Identify (MTTI). This denotes the average time it takes an analyst to identify an incident or intrusion. Chickowski [198] mentions that by reducing MTTD, analysts will give themselves more time to assess the situation and decide accordingly upon the best course of action. MTTD can be calculated using the formula shown in equation 4.1 [72]:

$$MTTD = \frac{1}{n}\sum_{t=1}^{n} DE_t \tag{4.1}$$

Where DE_t, is detection time, t is time, and n is a finite number of time it takes the analyst to detect an incident.

Another time-based performance metric suggested by Onwubiko and Ouazzane [72] is the Mean Time To Know (MTTK). According to the authors, MTTK comprises three components: *triage, isolation* and *diagnosis*. *Triage* is the time it takes an analyst to perform an initial assessment to ascertain whether the alert is a false positive or true positive. *Isolation*, they explain, denotes the identification of the origin of the attack or ownership of the source of the problem. Isolation in this context differs from removing an infected system from a network to reduce the spread of an incident. *Diagnosis*, which follows isolation, is the time it takes to conduct further analysis to ascertain the root

cause and recommend appropriate action. The formula for deducing MTTK is shown in equation 4.2 [72]:

$$MTTK = \frac{1}{n}\sum_{t=1}^{n} T_t + \frac{1}{n}\sum_{t=1}^{n} I_t + \frac{1}{n}\sum_{t=1}^{n} D_t \tag{4.2}$$

Where T_t represents triage time, I_t is the isolation time, and D_t is the diagnosis time. t is time, and n is a finite number of time it takes the analyst to complete each process successfully.

Another time-based performance metric discussed by Onwubiko and Ouazzane [72] is the time it takes the analysts to respond to an incident once it has been detected. They use the term Target Detection Time (TDT) which can be calculated as the delta between MTTK and MTTD, as illustrated in equation 4.3 [72]:

$$TDT = MTTK - MTTD \tag{4.3}$$

In a SOC where analysts are expected to apply a fix to rectify an incident, Mean Time To Fix (MTTF) an incident can be used to assess the performance of an analyst [72]. The formula for deducing MTTF is illustrated in equation 4.4 [72]:

$$MTTF = \frac{1}{n}\sum_{t=1}^{n} F_t \tag{4.4}$$

Where F_t represents the time it takes an analyst to fix or remedy an incident, t is time, and n is a finite number of time trials.

Mean Time To Verify (MTTV) and Mean Time To Resolve (MTTR) an incident is another time-based metric suggested by Onwubiko and Ouazzane [72]. MTTV denotes the average time it takes for an analyst to verify whether existing countermeasures or remedies applied to an incident have caused it to stop or whether mitigation has been

successfully applied. MTTR is the average time that it takes from when an incident is first detected to root cause analysis through to the resolution of the incident. Both MTTV and MTTR can also be deduced mathematically.

Onwubiko and Onwubiko [31] discuss a number of cyber KPIs that can be used to assess cyber security return on investment (RoSI). While their work focuses on providing metrics to measure organisational and national cyber security RoSI, many of their metrics are similar to those used when evaluating the performance of analysts, for example, the number of incidents detected [54] and the mean time to respond (MTTR) to an incident. Nugraha [28] also presents Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and Mean Time to Contain (MTTC) as useful metrics that can be used to assess the performance of SOC personnel.

There are also some subjective measures, such as the use of 'success stories' [54] and the quality of incident analysis and incident report [86]. However, subjective metrics (qualitative-based metrics) are seen by some writers as unreliable and advocate for them not to be used [196]. Nevertheless, some scholars, for example Hayden [128, p.35], take a different view and assert that qualitative-based metrics are equally as good as quantitative measures if they are based on empirical data.

Table 4.2 summarises the existing metrics used in a SOC for evaluating the performance of an analyst.

Table 4.2: Analysts' Performance Metrics as Reported in the Literature

Metric	Purpose
Mean Time To Detect (MTTD) an incident [25, 28, 39, 52, 54, 72, 86]. Also known as Mean Time To Tdentify (MTTI) [72].	It measures the delta between an incident occurring and a SOC analyst identifying the incident to raise a ticket. This metric is used to measure the average time that it takes for an analyst to identify an incident.
Mean Time To Respond [28, 52, 72].	Measures how long it takes a SOC analyst to respond to that incident and provide a mitigation action. In other words, the average time that it takes an analyst to stop and remediate a valid security incident.
Mean Time To Know (MTTK) [72].	This metric encompasses triage, isolation, and diagnosis. Triage refers to the initial assessment performed by analysts to ascertain the validity of an alert, distinguishing between false positives and true negatives.Isolation pertains to the accurate determination of the teams that have ownership of the source of the problem. The process of Diagnosis occurs after isolation and involves conducting a comprehensive analysis to ascertain the underlying cause and propose suitable remedies.

Table 4.2 – continued from previous page

Metric	Purpose
Mean Time To Fix (MTTF) [72].	This metric is used to measure the average time taken to implement appropriate remedies once the 'corrective actions' is known.
Mean Time To Verify (MTTV) [72].	This metric is used to measure the average time it takes for an analyst to verify whether existing countermeasures or remedies applied to an incident have caused it to stop or whether mitigation has been successfully applied.
Mean Time To Resolve (MTTR) [72].	This metric is used to measure the average time that it takes from when an incident is first detected to root cause analysis through to the resolution of the incident.
Time of Ticket Creation [25, 54, 56, 86].	This metric is used to measure the time it takes to create a ticket for an incident.
Time taken to Mitigate [56, 72].	This metric is used to measure the time it takes to mitigate an incident.
False Positives Detected [2, 39, 52, 91].	This metric tracks the number of false positives reported or identified by an analyst. The importance of this metric is that it enables a SOC to improve its tuning and filtering capabilities.

Table 4.2 – continued from previous page

Metric	Purpose
True Positives Detected [39, 52, 91].	This metric tracks the number of true positives reported or identified by an analyst. The importance of this metric is that it enables a SOC to demonstrate the detection of real incidents.
The number of vulnerabilities detected [31, 56].	This metric measures the number of vulnerabilities identified by an analyst.
The number of incidents closed [54, 56, 86].	This metric tracks the total number of cases opened against those pending. It is a useful metric for managers to assess how well incidents are handled.
The number of incidents detected [31, 39, 45, 52, 54, 56, 58, 86, 179].	The incidents that are raised amongst peers can be a useful way of identifying analysts that need training.
The number of indicators of compromised detected [31].	This metric tracks the total number of indicators of compromised detected by an analyst.
The quality of analysis [35, 91].	This metric is used to measure the quality of an incident analysis performed by an analyst.
The quality of an incident report [35, 86, 199].	This metric is used to measure the quality of an incident report written by an analyst.
The number of alerts/events analysed [35, 45, 86, 87, 91].	This metric counts the number of alerts analysed by an analyst.

It is possible to organise the metrics on Table 4.2 into three categories: 1) metrics that quantify the duration of time spent by individual analysts on each incident or ticket; 2) metrics quantifying the number of incidents or tickets processed; and 3) metrics that rely on subjective assessment, such as the quality of analysis.

The first two categories are objective metrics because they have quantifiable outcomes, for example counting the number of incidents raised by an analyst. The third category (subjective measurement), on the other hand, relies on human judgement of some kind. This can be problematic if there is no standard way of assessing performance when using subjective metrics. This study will seek to investigate how to define some guidelines in collaboration with SOC experts to establish standards for assessing subjective metrics. Also, the engagement with the SOC experts would provide the opportunity to identify and document metrics that were not captured in the literature.

4.5 Frameworks/Models for Performance Measurement

This section addresses research question 2 (RQ2): *"What frameworks and/or models exist for measuring the performance of an analyst? Is there a comprehensive framework, model or method for measuring performance?"*

Following a thorough and rigorous literature search, no formal framework was identified for measuring an analyst's performance. Also, no systematic method for evaluating an analyst's overall performance could be identified.

However, the literature search identified the work of Lif and Sommestad [147] which proposes a model for IDS operators and measurement methods for the human factors associated with the operations of IDS operators. The work of Lif and Sommestad [147] is of interest because it is closely related to the work of SOC analysts. Both IDS operators and SOC analysts support organisations in monitoring, analysing, and responding to cyber attacks. However, as acknowledged by Lif and Sommestad [147], the work of IDS operators is only a subset of the activities typically carried out by

analysts in a SOC. In the literature, there is evidence to suggest that in addition to these three functions, analysts are expected to perform a range of other functions, such as the management of vulnerabilities [56] and the application of patches [44]. In other words, the work of analysts is much more than monitoring, analysing, and responding to cyber threats.

Lif and Sommestad [147] identify how human factors such as attention, vigilance, automation, situation awareness, mental workload and multitasking impact the performance of IDS operators and suggest a number of techniques that could be used to assess these factors. In this context, human factors refer to how people interact with information, tasks, and business processes, as well as any associated human weaknesses that may lead to poor performance or unintentional harm to an organisation [200, 201, 202].

From the researcher's perspective, the absence of a framework or model for measuring the performance of an analyst could be attributed to factors such as a lack of clarity or comprehension of the actual responsibilities and duties of an analyst. Indeed, without a deep understanding of the functions of an analyst, it would be difficult to design a framework or systematic approach to measure their performance.

It is also probable that academic researchers have not managed to distil all the intricacies and variables needed to develop a comprehensive framework for evaluating the effectiveness of an analyst. Additionally, it is possible that researchers have not managed to obtain access to SOCs and SOC experts to engage them in order to develop a framework for measuring their performance. The development of a framework could be difficult if researchers lack access to domain expertise or the necessary data required for its construction.

Furthermore, it is also possible that there has been no demand for a framework because researchers and practitioners have not had the incentive, resources and time to develop one.

Despite the above, upon reflection from the researcher's perspective, the absence of

a framework or model for assessing an analyst's performance does not inherently imply that the development of such a framework is unattainable. This problem can be addressed by working with SOC experts and having a thorough understanding of any existing SOC framework and model useful for understanding the operations of a SOC.

Although the literature search did not identify a framework for assessing the performance of SOC analysts, two SOC frameworks were identified [21, 52]. This study contends that these two frameworks, along with the model in [147] can be used as the basis for building a new method for measuring the performance of an analyst. The two SOC frameworks are discussed in detail in Chapter 5 under Section 5.3.

4.6 Individual Performance Dimensions

As a part of the problem awareness phase, the literature was also searched to understand the areas of measures when assessing the performance of an analyst. An understanding of the areas of measures will aid with the suggestion and design of a new approach for measuring performance.

The search was guided by the research question 3 (RQ3): *"What performance dimensions and constructs need to be considered when evaluating analysts' performance?"*

The objective is to identify the existing measurable constructs or dimensions that could be used to evaluate an analyst's performance. The term 'dimension' in this context refers to the areas of individual analysts' work performance [12, 187].

To the best of the researcher's knowledge, the existing works on SOCs have not discussed the various areas of individual work performance measures when assessing an analyst's performance. To that end, the literature was explored to identify constructs or dimensions that could be taken into account when measuring individual work performance.

A literature review on the areas of individual work performance measures shows that a

variety of dimensions can be taken into account when assessing human performance in a work environment. However, most articles are concentrated in the fields of performance management, and organisational psychology [187]. Researchers such as Xu et al. [203] and Koopmans et al. [187] have conducted a systematic review on the dimensions of individual work performance.

According to Koopmans et al. [187], the main dimensions frequently cited by researchers to describe individual work performance in various disciplines are task performance, contextual performance, counterproductive work behaviour, and adaptive performance. Koopmans et al. [187] define the first dimension, *task performance*, as the proficiency with which one performs his or her central job tasks. The second dimension, *contextual performance*, according to the authors, refers to individual behaviours beyond his or her formal prescribed work goals - such as taking on an extra task, showing initiative or coaching newcomers on the job. Koopmans et al. [187] define *counterproductive work behaviour* as individual behaviours that harm the overall well-being of an organisation. They include behaviours such as absenteeism, being consistently late for work and engaging in off-task behaviour. The fourth dimension, *adaptive performance*, refers to the extent to which an individual adapts to changes in work roles or work systems. It includes, for example, learning new tasks, technologies, and processes.

Xu et al. [203] conducted a SLR within the process control domain and identified task performance as one of the main areas researchers focus on when measuring human performance. In addition to task performance, they also report on workload, situation awareness (SA), teamwork/collaboration, and plant performance (tools), as well as other cognitive performance indicators (OCPI), as the core areas of human performance measures frequently investigated by researchers assessing human performance in a work environment.

Like Koopmans et al. [187], even though the work by Xu et al. [203] is not within the domain of cyber security, the dimensions identified is domain-independent and can be used in different disciplines. For example, situation awareness and cognitive

performance indicators (such as attention) are studied in many other fields, such as air traffic control and psychology [204, 205]. Similarly, employee task performance has also been studied in the fields of management and psychology [187]. Therefore, the human performance dimensions discussed by Xu et al. [203] can be adapted and used in the context of a SOC when attempting to measure the performance of an analyst.

The definitions for the areas of human performance measures, suggested by Xu et al. [203], are as follows: *Tasks performance* - relates to an operator or team performance on a specified set of tasks. Koopmans et al. [187] explain that task performance includes work quantity, work quality, and job knowledge. *Workload* - refers to the amount of effort that an operator has to exert during an operation. *Situation Awareness* - relates to how an operator or a team perceives, comprehends, and predicts the status of elements relevant to the current operations. *Teamwork/collaboration* - is defined as an organised, collective working method between a group of people or between human-machine teams to collaborate and produce better quality results. *Plant performance* - refers to the extent to which a plant system's (or a tooling) outcomes, specified by an operator, meet the operational goals. In the context of a SOC, tools such as an IDS or SIEM represent systems that can be manipulated by an analyst to achieve their operational goals. *OCPI* - denotes constructs and measures that are not captured under the other five areas. OCPI encompasses the effectiveness of human information processing and metacognition, which is the awareness and understanding of one's thought processes.

The perception gleaned from the literature is that SOC managers often evaluate an analyst's performance based on the performance of their functions [49, 52, 54]. For example, SOC managers often use performance metrics such as opening and closing security incidents that focus on analysts' tasks to evaluate their performance [54]. However, as discussed in Section 4.4, there are several limitations with these kinds of performance measures, and as a result, prior works advocate for research that improves existing assessment methods [25, 54].

Xu et al. [203] posit that most studies that investigate human work performance

measures tend to focus only on some aspects of the six dimensions, as each dimension is a major field of research in its own right. Among the dimensions reviewed, task performance is the only dimension that was present in the work presented by both Xu et al. [203] and Koopmans et al. [187] in their systematic literature review on human performance dimensions.

This study recognises that, whereas the other areas are also important, task performance is often more measurable and objective than other aspects of human performance, such as counterproductive work behaviour [59]. Both quantitative and qualitative metrics can be used to assess task performance, making it easier to track progress. Indeed, the SLR on metrics for analysts shows that SOC managers prefer metrics based on task performance. Koopmans [59] explains that task performance represents an individual or team's performance on a specific set of tasks and objectives.

In a SOC setting, key objectives typically include goals such as the detection and reporting of attacks, as seen in the literature. Analysts' performance can be captured using effective metrics to ascertain how well they achieve set goals or objectives. Task performance is closely linked to the productivity of a business objective. Also, focusing on task performance will enable SOC managers to capture each analyst's contribution to the SOC's overall objectives.

Because this study focuses on analyst task performance, other dimensions such as contextual performance, adaptive performance, and workload would fall outside the scope of this research.

Even though task performance was selected as the focus of this study, the researcher recognises that it is just one aspect of overall human performance, and in certain situations, it may be necessary to measure performance from other dimensions, such as counterproductive work behaviours including absenteeism, complaining, and doing tasks incorrectly.

It is important to mention that this study did not seek to investigate the relationship

between the different dimensions creating an avenue for future work. Future work could consider investigating the relations between the dimensions and also how to capture analysts' performance from other dimensions.

This study argues that since the responsibilities of an analyst sit within the boundary of a SOC, it should be possible to use the existing SOC frameworks to build a conceptual framework to understand the operations of analysts and devise a new assessment method.

The next chapter presents analysis of the existing SOC frameworks that would serve as the foundation of building a new method for measuring an analyst's performance.

4.7 Chapter Summary - Conclusion

This chapter presented the state-of-the-art information on analysts' performance metrics. The evidence from the literature review revealed that, while performance metrics for analysts are of interest to cyber security researchers, more effort is needed to improve existing metrics to address the problems identified with current metrics. None of the papers examined present a systematic method of evaluating an analyst's performance.

There was a discussion of various dimensions for evaluating individual work performance. Among these dimensions, task performance was selected as the focus of this study. It is seen as an important dimension of individual work performance in several frameworks that measure human performance. Furthermore, focusing on analysts' task performance will enable SOC managers and supervisors to capture each analyst's contribution to the SOC's overall objectives.

The next chapter consolidates the existing SOC frameworks identified in the literature and argues that the existing SOC frameworks useful for understanding SOC operations could be used as the foundation for developing a new approach to measuring an analyst's performance.

Chapter 5

Leveraging the Existing SOC Frameworks and Studies to Build Innovative Artefacts

5.1 Introduction

This Chapter focuses on leveraging the existing SOC frameworks and models and using them as the foundation for building a new approach for measuring the performance of an analyst. The study argues that the existing SOC frameworks could be used to design a new approach for measuring an analyst's performance. The chapter concludes with a discussion on the challenges to designing metrics for analysts.

5.2 Formation Stage: The Building Blocks of a SOC Analyst Assessment Method

The search for a framework or model for measuring an analyst's performance in Chapter 4 revealed that currently, there is no existing framework, model or a systematic approach for evaluating an analyst's performance. However, the literature search showed that some frameworks and models exist for understanding the functions of a SOC and

improving the services offered by a SOC [21, 52]. This study proposes using the existing SOC frameworks as the basis for building a new approach for measuring an analyst's performance.

Dafikpaku [206] states that a framework is an outline or overview of interconnected items or activities designed to facilitate an approach to achieving a specific goal. Drawing on this understanding and the motivation to use existing SOC frameworks as the basis of building a new assessment method for analysts, the existing literature was searched to identify any SOC framework for understanding the overall functions of a SOC. Hevner et al. [144] explain that searching and exploring the literature for approaches that could be used to solve the practical problem is an important aspect of any DSR project. Guiding the search process were the following sets of research questions:

- *(RQ4) What frameworks exist for understanding the functions of a SOC and how could these frameworks be leveraged to design an approach for measuring the performance of an analyst?*
- *(RQ5) What are the challenges to devising effective performance metrics for SOC analysts?*

The methodology used to identify the existing SOC frameworks and models, is similar to the SLR process described in Chapter 4 under Section 4.3. The following electronic databases were used for the literature search: Scopus, the Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, the Association of Computing Machinery (ACM) Digital Library, Springer and Elsevier ScienceDirect. This was followed by literature searches using Google and Google Scholar. Both Google and Google Scholar were used with the intention of identifying any grey literature.

The search strings used are: ("security operations centre" OR "security operation centre" OR "security operations center" OR "security operation center") AND ("framework" OR "model" OR "functions" OR "security analyst" OR "challenges").

5.3 SOC Frameworks and Models

This section addresses research question 4 (RQ4): *"What frameworks exist for understanding the functions of a SOC and how could these frameworks be leveraged to design an approach for measuring the performance of an analyst?"*

The evidence from the literature shows that there is no standardised SOC framework. The absence of a standardised SOC framework has been well documented by cyber security researchers [21, 30, 50, 52, 57, 94, 207, 208]. Schinagl et al. [21] explain that the absence of a standardised framework for building a SOC has led to ad-hoc implementations, resulting in diverse SOC implementations and a high cost. Similarly, Jacobs et al. [30] noted an absence of appropriate classification schemes for assessing the efficiency and efficacy of SOCs, which they attributed to the lack of a standardised SOC framework. The direct consequence of not having a standardised SOC framework is that SOC implementations and functions differ between organisations, leading to variations in the role expected of an analyst [51]. Because there is no generally accepted SOC framework, this study opines that no single framework or model can be used as a guideline for building an assessment framework for SOC analysts.

Even though there is a lack of a standardised SOC framework, some cyber security researchers have developed frameworks for understanding the operations of a SOC and for improving the services offered by a SOC [21, 27, 52]. For example, the evidence from the literature suggests that in 2015, Schingal et al. [21] proposed what they called the building blocks for a SOC by modelling the structure of a SOC. In the same year, Onwubiko [52] also proposed a framework for understanding a SOC's operations. However, there were some differences in the SOC functions presented by the researchers. These differences are discussed in greater detail below.

Following the literature search, the frameworks by Schinagl et al. [21] (see Figure 5.1), and Onwubiko [52] (see Figure 5.2) were identified as the two main SOC frameworks. These findings have also been confirmed in a separate study by Majid and Ariffi [27].

The identification of SOC frameworks addresses Research Question 4 (RQ4), which seeks to uncover frameworks for understanding the functions of a SOC.

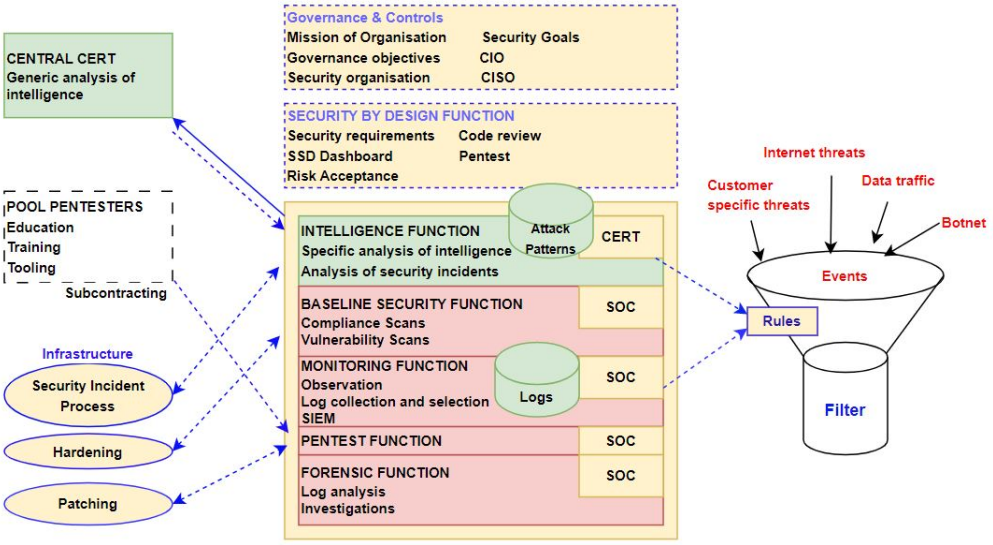

Figure 5.1: SOC Framework Proposed by Schinagl et al. [21]

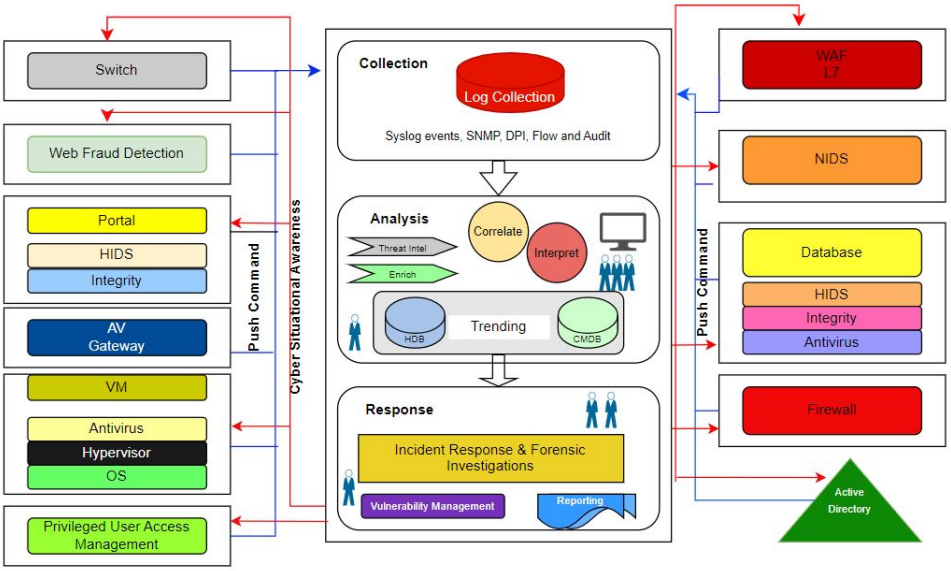

Figure 5.2: SOC Framework Proposed by Onwubiko [52]

Majid and Ariffi [27] discuss in detail the two SOC frameworks [21, 52] and highlight the similarities and differences between them (see Table 5.1). The two frameworks - Figure 5.1 and Figure 5.2 have in scope a monitoring and analysis capability. This

Table 5.1: A Framework of a Cyber Security Operation Centre [27]

Description	Schinagl et al. [21]	Onwubiko [52]
Approach and Research Methodology	Conduct a collaboration with VU University in Amsterdam. Uses Case Study method proposed by Robert K. Yin	Uses HMG Good Practice Guide (GPG13) - Protective monitoring for HMG ICT Systems as the basis of the study
Validation	Endorsed by the stakeholders in SOCs that participated in the study as well as the Netherlands Cyber Security Community.	Endorsed by representatives of SOCs in London
SOC Functions Reported in the Framework	Monitoring Function Threat of Intelligence Function Forensic Function Baseline Security Function Penetration Test Function	Collection Analysis Response and Forensic

similarity is important because many researchers have cited this function as a vital SOC activity [30, 147]. A description of these functions is presented in section 5.3.1 in Table 5.2.

A notable difference between the two SOC frameworks, pointed out by Majid and Ariffi [27], is that Onwubiko [52] does not include functions such as the penetration testing function, the intelligence function, or the baseline function. Onwubiko's framework's primary focus is on the monitoring, log collection function, the analysis function, and the response function. Onwubiko also mentions functions such as vulnerability management and the reporting function but does not discuss these functions in detail in the same manner as he does with the collection function, the monitoring function, the analysis function and the response function.

In contrast, the framework proposed by Schingal et al. [21] has almost all the functions listed by Onwubiko but with additional functions such as the threat intelligence function, a baseline security function, a penetration testing function and a forensics function. However, Schingal et al. do not mention the reporting function in their framework even though this function is well documented in a range of literature as a SOC's function [27, 44, 52, 92]. Taqafi et al. [15] also identify the functions suggested by Schinagl et al. [21] as the main SOC functional domains.

According to Majid and Ariffi [27], a possible reason why Onwubiko does not include the penetration testing and forensic function is that, in most cases, external third-party organisations tend to support an internal SOC with these functions. This view is consistent with the work of Jacobs et al. [30] that classifies penetration testing, vulnerability analysis and scanning as secondary SOC functions, as opposed to the primary function of a SOC. Nonetheless, it is important to emphasise that even when a third-party performs these functions, the SOC service will be delivered through a Managed Security Service Provider (MSSP) offering SOC services [79, 81]. An analyst may still have a role to play in fulfilling those functions, and therefore, a performance measurement framework would need to include them [55, 79].

In addition to the two SOC frameworks discussed above, the literature search also identified the work of Lif and Sommestad [147], which proposes a model for understanding the operations of Intrusion Detection System (IDS) operators. The model suggested by Lif and Sommestad [147] is discussed in Chapter 4 under Section 4.5. While Lif and Sommestad focus on IDS operators, they acknowledge the role of an IDS operator is a subset of what is expected of analysts working in a SOC. Therefore, their model is relevant to understanding the operations of an analyst. According to Lif and Sommestad [147], the primary functions of IDS operators are the monitoring function, the analysis function and the response function. These three functions also appear in the two SOC frameworks and are in agreement with previous studies that have sought to understand the functions of an analyst [46, 56].

The two SOC frameworks - Figures 5.1 [21] and 5.2 [52] and the three functional areas reported in the model for IDS operators proposed in [147] are consolidated in this research to build a list of the functions that one could expect of a SOC. This thesis uses the term "Global SOC Functions" to denote the consolidated functions [55]. In this study, "Global SOC Function" refers to the functions that could be offered by any organisation claiming to offer a SOC service. The consolidated SOC functions were subsequently validated by SOC experts to ascertain their completeness in terms of the functions offered by SOCs [55]. The objective is to validate the functions contained within the current frameworks and enhance them with recommendations from SOC practitioners.

The reasons for consolidating the frameworks and models are as follows:

- The framework proposed by Schingal et al. [21] is designed using case study research design as suggested by Robert K. Yin [150]. The authors claim that their framework is recognised by the Dutch security community as a model for designing and improving a SOC. The data for developing their framework came from observations, interviews, and workshops with SOC managers, analysts, and stakeholders. They also present SOC functions that are not covered by [147] and [52]. However, unlike Onwubiko, they omit incident reporting activities, which are considered an important SOC function [27, 30, 44, 52, 92].

- Even though the framework presented by Onwubiko [52] has some similarities to the framework proposed by Schingal et al., Onwubiko's work was carried out in a different context, in that no empirical data was collected from SOC experts. In fact, whereas Schingal et al. visited SOCs and collaborated with analysts and stakeholders through interviews and observations to develop their framework, the framework proposed by Onwubiko was designed by mapping the activities of a SOC against Her Majesty's Government (HMG) Protective Monitoring Controls (PMCs) [209], to illustrate how organisations can monitor their assets to understand how their IT systems are being used or abused.

- Finally, the model proposed by Lif and Sommestad [147], is also used due to the close similarities between the work of IDS operators and SOC analysts. In the literature, both analysts and IDS operators are expected to support an organisation to monitor, analyse and respond to cyber threats [147].

The two frameworks and the model, once consolidated and validated by SOC experts, were used as the foundation for the development of a conceptual framework depicting analysts' functions and the functions of a SOC. The conceptual framework was subsequently used to design a systematic method for measuring an analyst's performance.

5.3.1 Global SOC Functions

The amalgamation of the SOC functions identified in the existing works [21, 52, 147] resulted in ten functions as shown in Figure 5.3:

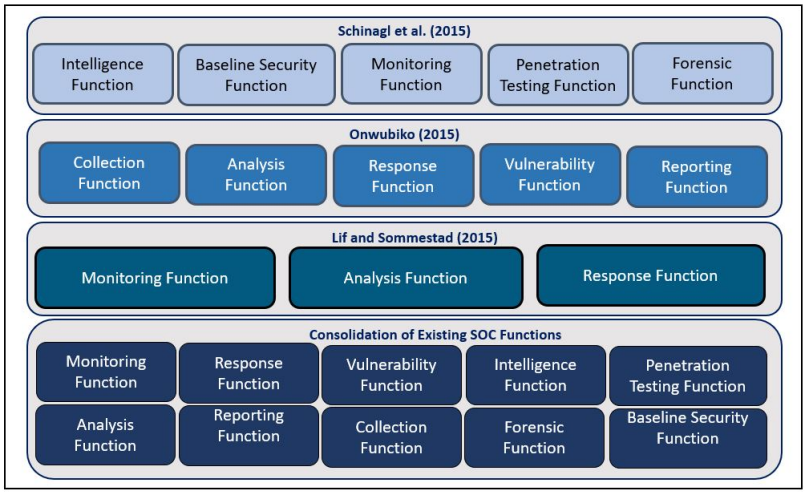

Figure 5.3: SOC Functional Areas

The table below summarises the functions as detailed in the literature.

Table 5.2: Functions of a SOC according to the existing SOC frameworks

Function	Description
The Monitoring Function	This is one of the primary functions of a SOC reported in the literature [21, 147]. Effective monitoring of an organisation's network by a SOC is achieved using security tools such as SIEM, IPS or IDS, which will trigger an alert when there are activities that match a pre-defined signature set signifying malicious activity [51, 54].
The Analysis Function	The trigger of security events marks the transition from the monitoring function to the analysis function [52, 147]. The analysis function is composed of a set of activities designed to conduct an in-depth investigation into observed abnormal activities, user behaviour, and incidents seen across an organisational network [21, 52, 210].

Table 5.2 – continued from previous page

Function	Description
The Response Function	To respond to cyber incidents and threats, many organisations maintain a cyber security incident response plan [211]. SOC services can be used to support businesses to achieve their cyber incident response strategy [21, 52]. The response function is generally accompanied by analysts' written reports, which detail the actions taken to address the reported issue, as well as the distribution of these reports to key stakeholders [210].
The Reporting Function	The reporting function usually involves notifying key stakeholders about cyber security incidents and creating an incident report for relevant stakeholders [27, 212]. Onwubiko [52] suggests that specific activities and expectations under the reporting function are driven by the service level agreements (SLAs) between the provider of the SOC services and the organisation that owns or is purchasing the SOC service.

Table 5.2 – continued from previous page

Function	Description
The Vulnerability Management Function	The vulnerability management function is concerned with identifying weaknesses in applications, services and network systems that an attacker could exploit to gain access to sensitive information [52]. Onwubiko [52] states that managing vulnerabilities in systems and preventing their exploitation can be achieved through an effective vulnerability management programme offered by a SOC.
The Baseline Security Function	Schinagl et al. [21] state that a SOC could be responsible for maintaining the operational effectiveness of all the hardware and software owned by an organisation and the hardening of these systems under the baseline security function. System hardening entails identifying and removing unnecessary services as well as closing all unused ports to improve the security posture of the organisation [21]. The baseline security function also ensures that an organisation's systems are patched to the appropriate level and that all systems running unsupported operating systems are identified [31].

Table 5.2 – continued from previous page

Function	Description
The Intelligence Function	The intelligence function involves the collection, sharing, and exchanging of cyber threat intelligence information between organisations [208]. Whereas SOC functions such as monitoring, analysis, and response are considered reactive services, the intelligence function is seen as a proactive activity [52]. Reactive functions do not actively seek to gather cyber threat intelligence information from various sources to defend an organisation's network against attacks [41, 52, 77]. On the other hand, proactive functions such as the intelligence function and the penetration testing function take a proactive approach to the defence of an enterprise network [52].
The Forensic Function	The forensic function enables businesses to identify, preserve, recover, analyse, and present digital evidence to establish digital crime [74]. This function has a lot of similarities to the analysis function as it entails the analysis of logs [21, 74]. However, unlike the analysis function, evidence collected from the forensic function could be used to prosecute the perpetrators of a crime [74].

Table 5.2 – continued from previous page

Function	Description
The Penetration Testing Function	The purpose of the penetration testing function is to simulate cyber attacks on the organisation's network to ascertain how the organisation would react in the event of a real attack by an adversary [21, 24]. The penetration testing function enables an organisation to gain a good understanding of their cyber-risk profile and to determine what can, or cannot, be breached [21]. Additionally, it helps organisations to determine the types of sensitive information that can be obtained once a system's defences are breached [24].
The Log Collection Function	To detect suspicious activity, SOCs collect security logs and data related to the systems they are protecting. Onwubiko [52] presents the log collection function in his framework and emphasises that log collection is a core function of a SOC. The log collection function offered by a SOC can also be used by businesses to meet regulatory and statutory requirements such as maintaining and archiving logs for a specific period [119].

The functions of a SOC discussed in the previous section can be used as the basis for understanding the work of analysts in a SOC and for developing a framework for

measuring the performance of an analyst.

These functions were presented to SOC experts during one-on-one interviews, and their opinions on the functions of analysts were solicited.

5.4 Challenges to Devising Performance Metrics

This section addresses research question 5 (RQ5), which investigates the challenges to developing performance metrics for a SOC analyst.

The evidence from the literature reveals that several factors hinder devising adequate performance metrics for analysts. Sundaramurthy et al. [25] mention that creating a useful performance metric is challenging because even SOC managers and stakeholders do not know what they need to measure to determine analysts' overall performance.

Another challenge to devising an adequate assessment method for an analyst is that every SOC is different, and analysts' expectations vary from one SOC to another [51]. According to Schingal et al. [21], each SOC is unique to the organisation it belongs to. This viewpoint is supported by McClain et al. [102], who state that different organisations conceptualise the work of analysts differently. As a result, the functions expected of the analysts vary from one SOC to the other; assessment methods need to consider the different functions.

Also, there is currently no agreement on what constitutes an analyst's core functions in a SOC [55, 57]. There is also no clear set of criteria on which an analyst's overall performance can be based [55, 212]. Even though cyber security researchers have discussed many of the functions and tasks expected of an analyst [25, 46, 54, 56], the evidence from the literature is that there is a lack of clear delineation on what constitutes the real functions of an analyst. In fact, D'Amico and Whitley [212] commented on the lack of any functional description of analysts' functions in their work on Computer Network Defence (CND) analysts.

Cyber security researchers often list various functions for analysts. For example, Andrade and Yoo [53] state that it is the responsibility of an analyst to monitor an organisation's network, identify threats, and fix vulnerabilities within the monitored network. However, they do not discuss tasks such as report writing and incident response activities, as suggested by other scholars [35, 44, 54, 56]. Graf and King [213] limit an analyst's tasks to threat identification and mitigation. On the other hand, Aung et al. [44] mention that analysts' functions also include finding critical security incidents, writing reports, and fixing or patching critical vulnerabilities.

Similarly, Kokulu et al. [56] state that analysts are expected to analyse network traffic and respond to security incidents, but they do not mention functions such as fixing vulnerabilities. Goodall et al. [51] say that the role of an analyst is to monitor an intrusion detection system for signs of malicious activity. Shah et al. [35] describe an analyst's functions as threat detection, analysis of security incidents, and reporting of incidents. According to Axon et al. [46], analysts' responsibilities include threat detection, triage of alerts, and responding to customer tickets.

The lack of consensus on what constitutes an analyst's functions means an attempt to develop an approach that can be used to measure an analyst's performance globally can be problematic. It remains unclear how complete the functions suggested in the literature are or whether the functions mentioned in the existing literature represent the most significant aspect of analysts' work upon which their performance could be based.

Islam and bin Mohd Rasad [60] state that an effective evaluation method for employees should be based upon sets of well-defined criteria that encompass the key aspects of their work. According to Islam and bin Mohd Rasad [60], if key aspects of an employee's function are ignored, employees could treat those aspects as less important. The problem is that, without identifying the most common and significant aspects of analysts' functions, it would be difficult to devise an evaluation method that can be used to measure analysts' performance globally. In other words, any performance metric is likely to be limited to local practice and cannot be used globally if the most common

and significant aspects of analysts' operations are not identified. For example, one SOC may offer a monitoring and detection function along with a reporting function but may not provide penetration or forensic analysis capability [30]. Likewise, some SOCs may offer compliance and vulnerability management functions but may not offer penetration testing or forensic analysis functions [21, 52]. As a contribution to the body of knowledge, this research formalises the functions expected of an analyst by working with SOC experts.

Another challenge to devising adequate performance metrics relates to the different tiers that operate in a SOC [56, 96]. Kokulu et al. [56] and Raimondi et al. [98] point out that most SOCs operate in tier structures, and analysts working at different tiers will often be expected to carry out different functions. Similarly, the same observation has also been made by other scholars [24, 54]. The responsibilities of analysts operating at different tiers can be blurred, which can cause a hindrance to devising metrics for analysts working at different tiers. These challenges need to be considered in order to create an approach that can be used to measure an analyst's overall performance.

This present study recognises the importance of an assessment approach that considers the different functions expected of an analyst operating in different SOCs. With this in mind, a tentative template representing SOC functions and metrics for analysts is devised (Appendix A) and Table 1 in Appendix B prior to engaging with SOC experts. The template was constructed using the template analysis technique proposed by King [148], which allows a researcher to define a priori theme as described in detail in Chapter 3. The tentative template was used during fieldwork involving empirical data collection from SOC stakeholders. The interview questions for the engagement is presented in Appendix B. The template consisted of the functions of a SOC from the existing SOC frameworks and metrics identified in the literature for each function.

The design of the template in Appendix A is based on the use of a hierarchical coding structure [148]. In this research, the hierarchical model used presents SOC functions at the top level of the hierarchy. The template seeks to establish the functions of a SOC

and the responsibilities of an analyst. The next level in the hierarchy seeks to establish the SOC role responsible for performing the SOC function presented in the hierarchy above. This is followed by a lower level of the hierarchy that presents a list of metrics under each function.

The second part of the hierarchy structure on the template has the theme of how to measure the performance of an analyst at the top. The levels below present the initial indicators that must be present in a quality analysis and an incident report.

The goal of the template was to simplify the extraction of an analyst's responsibilities across SOC functions and to elicit from the SOC experts functions and responsibilities missing from the template. Also, engaging with SOC analysts is important because an assessment method that does not incorporate their perspective is bound to face resistance from analysts themselves according to Sundaramurthy et al. [25]. Furthermore, Sundaramurthy et al. [29] argue that analysts will perceive performance metrics that are devised without analysts' involvement as flawed. Islam and bin Mohd Rasad [60] state that employees (analysts) are more likely to accept the outcome of an assessment if they are involved in the way it is designed, even if the outcome is adverse. This viewpoint is supported by Deadrick and Garner [214], who assert that employees will perceive an evaluation system as fair if they are involved in how it was designed.

Islam and bin Mohd Rasad [60] state that an effective evaluation system must have a set of well-defined criteria. This study contends that the primary functions of an analyst, as suggested by SOC experts and found in the existing SOC framework, can be used to devise a method to measure analyst performance. In other words, the goal is to measure an analyst's performance by focusing on the main work of analysts as identified in the literature and through the study's engagement with SOC experts. This is in line with the suggestion by O'Connell and Choong [61], who state that performance metrics must focus on analysts' real-life workplace needs.

5.5 Chapter Summary- Conclusion

This chapter presented a detailed discussion of the existing SOC frameworks and models that were used as the foundation for developing a systematic method for measuring an analyst's overall performance. The chapter also presented the challenges to devising effective metrics for analysts that could be used in different SOC settings. The next chapter presents empirical case studies, data analysis and artefacts designed to facilitate the assessment of analysts' performance.

Chapter 6

Case Studies, Data Analysis and Artefacts Design

6.1 Introduction

This chapter provides a detailed description of the empirical data collected from the SOC experts, the analysis of the collected data and its findings as well as the artefacts that were developed. In Chapter 3 the DSR process along with a case study was identified as the methodology for designing, building and evaluating an artefact to solve the research problem. The central research question driving the engagement with the SOC experts was:

(RQ6) How could the performance of an analyst be measured in a systematic manner addressing the drawbacks of existing methods?

6.2 Iteration 1- Constructs and the SOC Conceptual Framework

Twelve (12) SOC experts, which comprised eight (8) SOC analysts and four (4) SOC managers, participated in a one-to-one semi-structured interview. 17% (2 out of 12) of the participants were female, and 83% (10 out of 12) were male. The participants

had varying levels of expertise and years of experience working in a SOC; the average years of experience was over six years. Table 6.1 presents the participants' demographic information (Interviewee ID, job title, gender, type of industry and years of experience).

Table 6.1: Interview Participants' Profile and Organisation

Interviewee_ID	Job Title	Gender	Industry	Years of Expereince	Participated in the Delphi Study ? (Y/N)
P1	Senior Analyst	Female	Airline	8	N
P2	SOC Manager	Male	Airline	5	N
P3	SOC Analyst	Male	Defence	5	N
P4	Senior Analyst	Male	Defence	9	N
P5	SOC Manager	Male	MSSP	14	N
P6	SOC Analyst	Male	Defence	5	N
P7	SOC Analyst	Male	Airline	4	Y (Delphi Study Participant 3)
P8	Senior Analyst	Female	Defence	6	N
P9	SOC Manager	Female	Airline	2	N
P10	SOC Consultant	Male	Finance	7	Y (Delphi Study Participant 2)
P11	Cyber Operations Specialist	Male	Telecom	5	Y (Delphi Study Participant 4)
P12	Cyber Incident Director and Deputy Head of Security Operations	Male	Automobile	10	Y (Delphi Study Participant 6)

An invitation requesting SOC experts to participate in this research was initially sent to analysts of the organisation supporting this study. Analysts who expressed interest in participating in the interview made referrals to other analysts working in different SOC settings and industries. Invitations were sent to those referrals. As explained in Chapter 3 under Section 3.5, the study's participants were 'purposively' selected because they had relevant experience and/or unique insight about the issues under study [137].

It is important to point out that the final number of participants (12) was not predetermined at the outset of the study. Instead, the objective was to conduct interviews with as many SOC experts as feasible until the point of saturation, which refers to the stage where no new information is being revealed [215]. Achieving a'saturation point' is an important validation technique in qualitative research [64, 215], as discussed in Chapter 3. It is also important to acknowledge that, despite reaching 'saturation point' after nine interviews, a decision was made to conduct interviews with the remaining experts who had already indicated their interest in taking part in the study.

To ensure a meaningful discussion with the participants, each participant was provided

with an interview pack containing participants briefing sheet, a consent form, and a template describing SOC functions and useful metrics for capturing performance under each function (See Appendix - O for the interview consent form and the participants briefing sheet). Table 1 in Appendix B contains the template used as part of the interview. The template was devised using insight from the existing SOC frameworks and model [21, 52, 147]. All the interviews were conducted face-to-face, with each interview lasting approximately an hour.

The objectives of the interview were to (1) identify and validate the functions of an analyst among the range of SOC functions, (2) identify appropriate metrics for evaluating analysts' performance, and (3) investigate how to improve the evaluation method for analysts.

6.2.1 Discussion of Findings

The interviews were taped and transcribed, resulting in over 100 pages of interview transcripts. The interviews transcripts can be found in the following location:

https://git.cardiff.ac.uk/c1854157/interviews-transcripts.git

The qualitative NVivo 12 software was used to organise the transcripts. The data was analysed using the TA technique [148] as described in the methodology chapter. The TA allows researchers to use direct quotations and paraphrases from the participants' responses during the discussion of the research findings [148].

The themes developed as a result of the interviews, observations and the document reviews are presented in Appendix C and the detailed discussion of these themes are presented below.

The themes are organised into four major areas: (1) the functions of an analyst, (2) non-analyst SOC functions (additional SOC functions), (3) metrics for analysts and (4) how the performance of an analyst should be measured. The themes are presented

below. Direct quotations and paraphrases from the participants' responses are used during the discussion of the research findings as a part of the TA application [148].

6.2.2 Theme 1: The Main Functions of an Analyst

The first theme relates to the functions of an analyst. The following were suggested by participants as the functions of an analyst: (1) monitoring and detection function, (2) analysis function, (3) response and reporting function, (4) intelligence function, (5) incident management function, (6) baseline and vulnerability management function, (7) policy and signature management function and (8) Compliance and Risk Management. These functions and their descriptions serve as 'constructs' regarding the functions of a SOC analyst [144]. The sections below present the functions as suggested by the study participants. The suggestions also confirmed and validated the functions identified in the existing SOC frameworks.

6.2.2.1 Monitoring and Detection Function

The participants described the monitoring and detection function as one of the primary functions of an analyst. Participants discussed in detail the responsibilities and expectations of analysts under this function. For example, P5, a SOC manager with fourteen years of SOC experience, stated *"the monitoring and detection function is the main responsibility of a SOC analyst."* A similar view was expressed by P3, who articulated that analysts *"monitor network traffic and triage accordingly. They then analyse it and decide where it needs to go."* Triage is the initial check conducted by analysts to determine whether the alert is a false positive or true negative [72]. Triage also involves classifying incidents according to their priority or severity level [2, 71].

P2 and P6 indicated that analysts monitor an organisation's network by observing the sequences of activities over the network using various tools. According to P10 and

P11, analysts aim to identify external attackers or privileged users engaging in illegal activities that contravene the organisation's security policies.

The findings from the above are in agreement with existing works on SOCs, which suggest that analysts play an important role in monitoring an organisation's network [29, 51, 53]. For example, Onwubiko [52] states that an analyst plays a vital role by monitoring an organisation's network in order to detect cyber threats and incidents. In fact, the description provided by the participants confirmed what Onwubiko [52] describes as analysis providing "eyes on glass" monitoring of an organisation's computer network systems and the applications running on those systems. A recent study by Mário and Coelho [16] also state that the majority of a security analyst's time in a SOC is dedicated to the monitoring and detection of cyber threats.

Participants P10, P11 emphasised the importance of the monitoring and detection function and argued that an evaluation method for analysts must take their performance under this function into account.

6.2.2.2 Analysis Function

The Analysis Function is recognised as a core function of a SOC by the SOC frameworks and the model. This function has also been documented as a SOC activity in [21, 27, 38, 52, 56, 92, 216].

Participants stated that much of an analyst's work focuses on analysing security events and logs to identify malicious activity on a network (P1, P2, P4). Participants discussed in detail how analysts perform their analysis function to identify signs of malicious activity within the logs. For example, P1, an analyst with eight years of SOC experience who works for an airline SOC, said, *"I definitely think the analysis function is the most important function. It is also our primary role as security analysts."* Another participant, P3, a SOC analyst working in the defence industry, stated that *"analysts must analyse all traffic and packets to know what is going on across the organisation's network."*

P6 echoed a similar point. P6 articulated that *"analysing log files allows analysts to identify security incidents."* P11 stated, *"analysts should be able to analyse an alert to determine if it is a false positive, false negative, and where it falls in the scope of their activities"*. P8 asserted, *"the monitoring and detection, the response and reporting, are all underpinned by good analysis."*

The participants' descriptions of how an analyst conducts their analysis were also consistent with D'Amico and Whitley's [212] discussion of the data triage analysis. Data triage analysis, which is also referred to as 'alert analysis' by some writers [91, 199], entails examining the details of data sources such as IDS alerts to remove false positives and identify a real attack. An unexpected finding was that almost all of the participants favour basing analyst performance on the quality of their incident analysis.

6.2.2.3 Response and Reporting Function

The participants emphasised the importance of this function and described that the response and reporting function go hand in hand. P3 commented that *"there is no point in monitoring an organisation's network if analysts are not going to respond and report unusual or abnormal network activity."* According to participant P3, monitoring and detection, analysing network traffic, and responding to cyber threats are very much interrelated in that you cannot have one without the other. P1 agreed with this point of view. P1 stated that the response and reporting functions are inextricably linked with the analysis function because analysts report an incident based on their analysis of an observed event.

The participants explained that analysts need to respond to security incidents by following their organisational processes in order to reduce the impact of identified threats (P1, P4, P7). These comments are consistent with suggestions in the existing literature, which state that analysts are expected to take actions mandated by their local working processes to mitigate threats [51, 52, 147]. Participants asserted that the response

function must be accompanied by security incident reports to relevant stakeholders on incidents (P1, P7, P11). This finding confirms insight from the existing work suggesting that the reporting function usually involves notifying key stakeholders about cyber security incidents and creating an incident report for relevant stakeholders [27, 212]. The findings also confirms the work by Zhong et al. [199] who point out that analysts are expected to produce a timely and high-quality incident report.

6.2.2.4 Intelligence Function

Participants described the responsibilities of analysts in this function, explaining that analysts are expected to 'hunt' for threats and gather threat intelligence from external sources on a proactive basis (P10, P11, P12). P12 stated that analysts use threat intelligence from a variety of sources, including vendors and other security agencies, to re-configure their security solutions in order to protect an organisation's network. P12 went on to say that analysts rely on cyber threat intelligence information sharing from trusted parties to spot unusual network activity that may not be obvious. This statement supports the literature's view that the intelligence function is a proactive activity carried out by analysts in anticipation of attacks before they occur [212]. The findings from the participants also confirms what Majid et al. [208] described in their work as the intelligence function involving analysts collecting, sharing, and exchanging cyber threat intelligence information with other organisations.

According to participant P10, analysts are expected to collect information on indicators of compromise (IOCs) and indicators of attacks (IOAs) from third parties and open sources to develop use cases that can then be employed to detect malicious activities. P10's statement was corroborated by P8, a SOC analyst in the defence industry. *"You can't monitor and detect emerging threats if you don't have intelligence feeding your monitoring and detection tools."* To detect cyber attacks, an analyst is expected to gather threat intelligence information, create use cases, and feed that information into their monitoring tools (P5).

6.2.2.5 Incident Management Function

Another function of a SOC analyst, according to participants P1, P5, and P10, is incident management. This was surprising because this function is not mentioned in any of the existing SOC frameworks. However, further insight from interview data and confirmed by the participants through the member check, revealed that an incident management function is not a distinct function by itself but rather an activity carried out as part of the monitoring, analysis, and response to a cyber threat. P1 stated, for example, that *"an incident management function underpins the monitoring, analysis, and reporting of a cyber threat."* This view from P1 is in-line with the work of Miloslavskaya [76], who described the activities of incident handling as consisting of detecting, notification, responding, and reporting. Likewise, Jacobs et al. [30] also state that incident management is the ability to prepare, identify, and escalate an incident.

Based on the above findings, this study argues that an analyst's performance under an incident management function can be derived from their efforts in monitoring, analysing, and responding to cyber threats. However, further research may be required to investigate and understand the relationship between these functions.

6.2.2.6 Baseline and Vulnerability Function

Participants stated that an analyst could be expected to perform system vulnerability scanning to identify weaknesses (P1, P10, P11). They may also be expected to ensure that an organisation's systems are baselined by ensuring that computer systems adhere to a basic security objective. The perception gleaned from the literature is that the activities of baseline functions are very similar to those performed under the vulnerability management function [21]. Indeed, the description of vulnerability management functions by Onwubiko [52] is similar to what Schinagl et al. [21] call the baseline security function. Schinagl et al. [21] treat vulnerability management activity as a subset of the baseline and security function.

Participants also mentioned that as a part of vulnerability management, analysts perform patching and hardening of systems to address known flaws in the system (P3, P4, P6, P7). These findings are consistent with the work by Aung et al. [44], who mentioned that analysts are expected, in some cases, to fix vulnerabilities. Likewise, Andrade and Yoo [53] also state that analysts are responsible for fixing vulnerabilities.

According to P11, an analyst's responsibility in the baseline and vulnerability function is to ensure that an organisation's network systems are up to date and that patches are rolled out as soon as the vendor releases them. P11 went on to say, *"You should be able to keep your network up to date; you should be able to patch everything; you should know what is going on."*

6.2.2.7 Policy and Signature Management Function

Another function of an analyst described by the participants is the policy and signature management function. The security tools such as SIEM, IDS, and IPS used by SOCs come with security signatures and policies, also known as "use cases", that are used to detect cyber threats. Participants mentioned that analysts play a vital role in maintaining the use cases and signatures on these technical tools (P8, P10). According to P10, poor use case and signature management can lead to increased false positives, which puts pressure on analysts. P10 further explained that analysts must ensure that the signatures and policies are tuned to reduce false positives that can impede their ability to identify real incidents.

Both P10 and P11 stated that an analyst's responsibilities under the policy and signature management include: maintaining, amending, changing, and creating use cases for SIEM tools. P4 articulated, *"for me, even though it is not something that I do a lot of, I consider policy management as the most important function of a SOC... because without correct rules and tuning, it is just not possible, and you are just looking at false-positives all the time, it's just noise."*

Participant P8 articulated, *"if you say your policy management is not important, your monitoring and detection will fail because you are not managing the tools you are using for the monitoring."* According to P10, *"everything the SOC does comes back to policy management because if you don't have a policy and don't have the rules and use cases to pick up risk, what is the point of the monitoring?"* However, surprisingly, existing frameworks do not discuss signature and policy management.

6.2.2.8 Compliance and Risk Management Function

Participants (P10, P11, and P12) also mentioned compliance and risk management activity as a function of a SOC. However, none of the existing SOC frameworks suggested this as a SOC function. Analysis of the interview data revealed that only participants P10, P11, and P12 mentioned this as an analyst's function.

P10 asserted that organisations need to understand the legal ramifications of their activities. P10 (a SOC consultant who works within the financial sector) explained that within the financial industry, organisations could be audited and penalised for failing to comply with, for example, data and privacy laws because of the nature of the information they handle under the European Union General Data Protection Regulation (GDPR) or PCI-DSS.

P11 stated that understanding the risk a business faces is crucial because it allows analysts to understand where they are contractually required to have use cases. P10 stated, *"if analysts do not know a business's risks, they cannot create effective use cases to mitigate the risk."*

Participants P10 and P11 explained that a SOC providing compliance and risk management functions must collaborate closely with the business to identify where the risk lies, what can be done to mitigate the risk, and to address any regulatory or statutory requirements. These views confirm the statement by Miloslavskaya [76], that a SOC can support a business to identify the risks they face and rank these risks based on the

Business Impact Analysis (BIA). Similarly, in [217] risk assessment is identified as one of the functions of a SOC.

6.2.3 Theme 2: Additional SOC Functions

The second theme relates to the SOC functions that are not performed by analysts. Even though existing SOC frameworks [21, 52] present: (1) penetration testing, (2) forensic and malware and (3) engineering and log collection functions as SOC functions, the findings from this study reveal that these functions fall outside the remit of an analyst. While these functions are not performed by analyst, they are presented here as part of the study findings to further confirm the functions of a SOC in general.

6.2.3.1 Penetration Testing Function

The participants indicated that their SOC supports penetration testing activity. The penetration testing function involves simulating cyber attacks against an organisation's computer network systems to test its defences and how it will respond when attacked [21]. However, the participants mentioned that the penetration testing function was carried out by professionals other than analysts. For example, P10 and P11 stated that their SOCs employed a specialist team of penetration testers to carry out this function.

When describing the penetration testing function, P10, a SOC consultant at one of the UK's largest banks, stated that:

"Analysts do not do penetration testing; instead, we get an outside team to do it. We also have an internal pentest team who sits alongside the SOC. We carry out regular purple team activity where they will do testing, where another external team will also come and do testing, which then feeds back into the framework that you have here because then they can identify the areas which are at risk, obviously to write new use cases, new rules, and so on."

P11 explained that a SOC needs penetration testers and red teams to work collaboratively with analysts in order to be able to deal with emerging threats. According to P11, one way of knowing your vulnerabilities and patching status is through red team and penetration testing activities. P11 pointed out a distinction between the red team and penetration testing: the mission of a red team is usually more narrow in focus in comparison to pentesters. Red teams seek to focus on exploiting a specific vulnerability using physical or electronic social engineering. Therefore, the penetration testing function will be excluded from the proposed measurement method because it is not an analyst's function.

6.2.3.2 Forensic and Malware Function

Participants (P3, P9, P10, and P12) mentioned the forensic and malware function as one of the functions of a SOC. According to the participants, the forensic and malware function entails gathering and preserving evidence relating to malicious activities in a manner that is acceptable to a court of law (P10, P12). The comments from the participants were consistent with the view expressed by Miloslavskaya [76], who states that the forensic capability offered by a SOC can be used to identify, gather, preserve, recover and present facts related to a cybercriminal incident.

An observation from the interview data is that, even though some authors mention that analysts could perform a forensic investigation [74], participants suggested that the forensic and malware capability function is performed by a specialist professional and not by an analyst. For example, P3 mentioned that the forensic and malware functions are carried out by a specialist team that works closely with law enforcement agencies. A similar view was expressed by P10, who articulated that *"we have a forensic specialist in our team who analyses our malware and forensic data."* The suggestions from the participants on the use of a specialist team to address forensic and malware functions is aligned with the work by McClain et al. [102], who state that a specialist team is required to undertake the forensic analysis. This view is also supported by the work of

Mário and Coelho [16].

The Forensic function is not one of the main functions of an analyst and is a function typically delivered by a forensic expert. Therefore, this function will be excluded from the proposed measurement method.

6.2.3.3 Engineering and Log Collection Function

Another SOC function reported in the existing literature [52] and confirmed by the study participants is the engineering and log collection function. Participant P5 stated that detecting attacks would be impossible if a SOC did not collect, manage, and maintain security logs from their network. Onwubiko and Ouazzane [38] state that in order to collect logs, security tools and endpoint devices, they must first be onboarded into security information and event management systems by SOC engineers and solutions architects. The findings from this research support the statement by Onwubiko and Ouazzane in that participants, for example, P10, reported that it is SOC engineers and not analysts that conduct the log collection functions. Similarly, the participants explained that engineering activities such as tuning of systems are the responsibilities of SOC engineers and not analysts. The consensus among the participants was that this function is outside the scope of an analyst's function. As a result, the proposed evaluation method will not include this function.

6.2.4 Theme 3: Performance Metrics for SOC Analysts

The third theme concerns metrics for analysts. Participants suggested a number of metrics for measuring the performance of a SOC analyst. The metrics suggested by the participants can be grouped into two categories: quantitative metrics and qualitative metrics. The quantitative metrics comprise cardinal numbers and time-based. Whereas the time-based metrics reflect the time it takes an analyst to perform an activity; cardinal numbers are based on counting the number of times an analyst performs a particular

SOC task. A cardinal number is a number that is used to denote how many of something there are, starting from 1 and increasing sequentially such as 1,2,3,4,5, without fractions or decimals [196]. In [196], the author opines that good metrics should be expressed as a number or percentage. The section below describes the different metrics suggested by the participants.

6.2.4.1 Quantitative Metrics: Cardinal Numbers

The number of incidents raised and/or closed by an analyst was reported by some participants as a useful way of measuring their performance (P7, P11). However, some participants expressed reservations about using cardinal numbers such as the number of incidents raised as an indicator of performance. P1 stated, *"I am not entirely sure on the use of numbers because what happens if there is nothing to raise; how can analysts be measured on that?"* P11 stated that *"if you've got a very quiet network, analysts may not raise many incidents."* Nonetheless, researchers [196] state that good metrics should be expressed as a number or percentage. The numbers they mention should be a cardinal number - something that counts how many of something there are.

Some of the participants also opined that measuring analysts' performance solely on the number of incidents raised or closed does not give the full picture of the work expected of an analyst (P1, P4). This finding is similar to what has been reported in the literature [56]. P4 commented, *"every situation is different. Measuring analysts' performance solely on numbers doesn't provide the whole picture, but it is a starting point, as there are other tasks that they do."* The concerns and reservations from some of the participants call for the need to explore other ways of measuring analysts' performance besides the use of cardinal numbers.

Even though some of the participants expressed concerns about using cardinal numbers as an indicator of an analyst's performance, others, such as P6 and P11, believed that one cannot remove numbers as a measure of an analyst's performance. P6 stated that

"you don't want a small group of analysts doing a huge proportion of the work and others doing very little."

While the use of cardinal numbers as an indicator of performance seems to be a straightforward metric, Jaquith [196, p. 22] opines that metrics based on cardinal numbers are good metrics. Jaquith contends that metrics that are not expressed in numbers do not qualify as good metrics [196, p. 24]. However, scholars such as Hayden [128, p.35] oppose such an assertion. Hayden [128] states a metric does not have to be a number to qualify as a good metric. From Hayden's perspective, qualitative metrics are equally as good as quantitative metrics if they are based on empirical observations and experience. This study takes the position of Hayden [128] and argues that both qualitative and quantitative metrics can be used to evaluate performance if it is based on empirical observation and experience.

6.2.4.2 Quantitative Metrics: Time-based

The participants also suggested a number of time-based metrics for analysts. P11 stated that an analyst's performance could be assessed based on how long it takes for him/her to open an incident from a system and how long it takes them to investigate an incident. P1 also mentioned the time it takes an analyst to investigate an incident as a useful metric.

P1 and P3 mentioned the time to detect as a useful metric when seeking to measure performance. Another time-based metric suggested by the participants was the time taken to mitigate an incident. This metric is used to determine how quickly an analyst implements, or recommends, a mitigation action that can stop or slow down an active threat. P12 also mentioned "time to response" as a metric for measuring the amount of time it takes for an analyst to confirm that an incident has been investigated and mitigated [72].

According to P8, one advantage of using time-based metrics is that managers can know

how quickly analysts are reacting to incidents. However, P8 argued that *"if an analyst is taking too long to respond to things, you can't tell them to respond faster if they are overloaded."*

While participants mentioned time-based metrics, the consensus among the interviewees was that time-based measures are often misleading and should not be used to indicate an analyst's performance because there are too many factors beyond an analyst's control. This statement has been reported by other scholars such as Chamkar et al. [39]. For example, P10 commented that a complex incident could take a lot of time. Similarly, P2 stated, *"the time taken to perform an activity has so many variables. There could be external factors. I wouldn't judge analysts based on how quickly they raise an incident."* Likewise, P4 stated *"time-based metrics do not consider the type of incident."* P7 opined that metrics such as *"time of ticket creation doesn't give the full picture."* These findings are also consistent with the statement made by Vielberth et al. [57] that the analysis work of analysts can take minutes or hours to complete.

The problem with time-based metrics suggested by the participants is consistent with what has been documented in prior work relating to time-based metrics [72, 91]. For example, Onwubiko and Ouazzane [72] point out that the time taken to detect an incident can be affected by several factors, such as monitoring system configuration or the processing power of the sensors sending the alerts. Shah et al. [91] also take a similar view and emphasise that time spent by analysts would vary between shifts, depending on the variation in alert arrival time.

6.2.4.3 Qualitative Metrics

Five participants also suggested a number of subjective metrics, such as the quality of incident analysis and the quality of an incident report (P5, P6, P7, P10, P12). P4 asserted, *"quantitative-based metrics such as the number of incidents raised by an analyst alone does not take into account the level of analysis you have to go into. It's the quality of the work you do as well; the write-up and everything."* These statements

are in alignment with the work by Kokulu et al. [56], who suggest the limitations of quantitative metrics.

Another problem associated with qualitative metrics, such as the quality of analysis, is that understanding of what the term "quality" means will vary from one person to another. According to P1, the only way to establish the quality of incident analysis is to check the report they produce. P11 said, *"nobody can see what is going on in the mind of an analyst, or anybody else unless they report it."* P11 mentioned that the quality of analysis should be based on the way they are reporting their analysis. This research argues that guidelines can be provided to address this issue.

6.2.5 SOC Conceptual Framework

The constructs were organised into the SOC conceptual framework shown in Figure 6.1 based on the insights from the analysis of the interview data. The framework was validated by the SOC experts (see Chapter 7) as a useful framework that can be used to develop an approach for capturing the performance of an analyst. The framework is presented in [55]. The term "Global SOC functions" is used in research to represent the eleven functions, as these represent the services that can be expected from a SOC based on insight from existing research [21, 27, 52] and the findings from this empirical study.

The top half of the Figure 6.1, shown in the red dotted lines, represents the primary functions of a SOC. Studies also suggest that these are the most critical areas of a SOC [208]. The red arrow between the yellow and pink boxes indicates that the monitoring and detection activity is immediately followed by responding and reporting. Underpinning the "monitor and detect", "respond and report" is the "analysis function" shown in the grey box. The metrics reported by participants as relevant to the assessment of analysts are represented in the orange box (qualitative and quantitative-based metrics). The purple box within the red dotted lines illustrates the main metrics suggested by participants as vital to capturing the performance of analysts in a SOC. The functions in

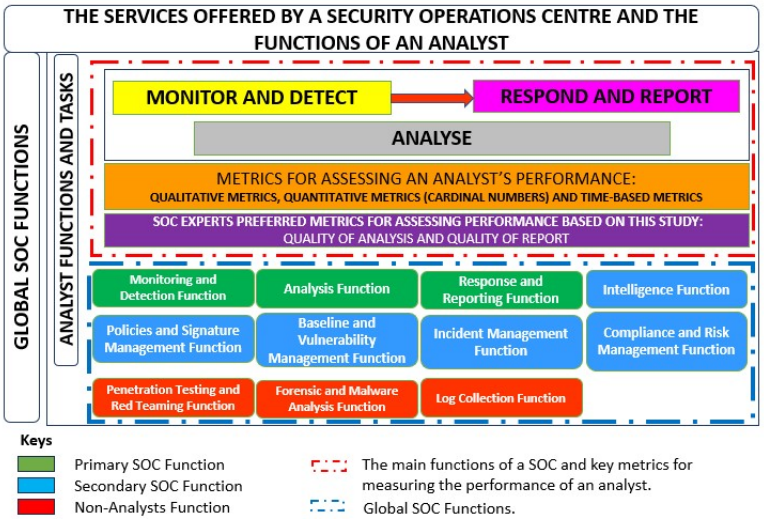

Figure 6.1: SOC Conceptual Framework [55]

the red boxes at the bottom half of the framework are functions that are not performed by analysts but by a specialist team.

6.3 Iteration 2 - Development of the Security Operations Centre Analysts Assessment Framework (SOC-AAF)

6.3.1 SOC-AAF

The SOC conceptual framework from iteration 1 was used to design the SOC-AAF (Figure 6.2). The SOC-AAF contains only the functions of analysts as suggested by the participants. Two criteria were used for the design of the SOC-AAF:

1. The SOC functions included in the SOC-AAF must either be present in the existing SOC frameworks [21, 27, 52, 208] and validated by the study participants as a function of an analyst; or it must be a SOC function performed by an analyst

function that is not in the existing frameworks but are suggested by the study participants.

2. The function must have metrics for measuring an analyst's performance based on the findings from the existing literature or recommendations from the research participants.

Both criteria must be true to be included in the SOC-AAF.

The SOC-AAF maps various metrics to the analysts' functions suggested by the participants. It is important to point out that SOC functions such as penetrating testing, which analysts do not perform are not shown in the SOC-AAF. Also, the incident management function is not present because it underpins the monitoring, analysis and reporting function and is not a separate function per se based on this study's findings. Also, the literature review did not identify metrics for the compliance and risk management function and the participants did not mention any specific metric that could be used to measure performance under this function. To that end, this function is not included in the SOC-AAF.

Under the SOC-AAF, while an analyst's performance can be individually assessed under each function, as shown in (see Figure 6.2), it does not allow for the aggregation of the overall performance. This limitation necessitates the need for a third iteration of the DSR process to find a way of solving this problem.

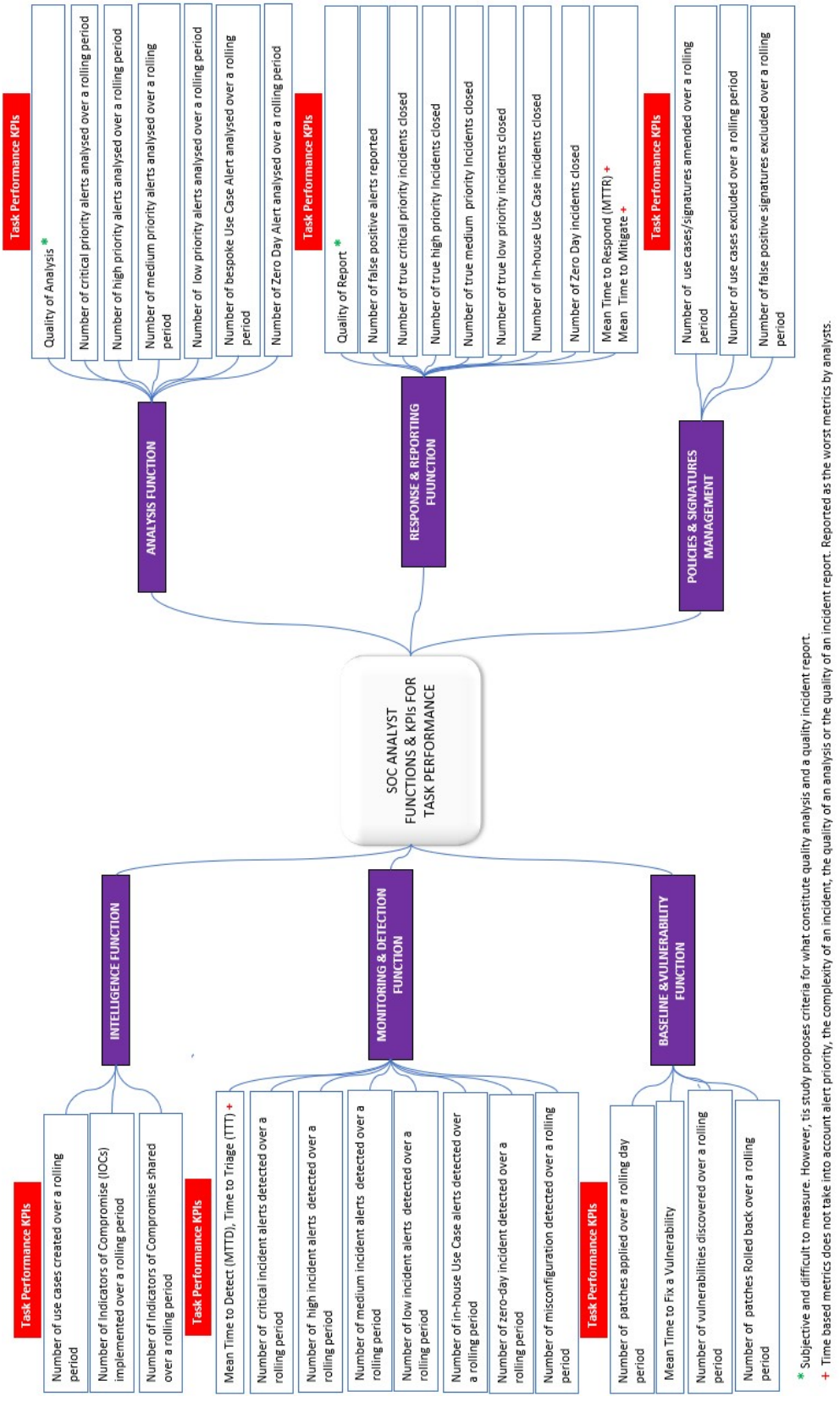

Figure 6.2: SOC-AAF

6.3.2 Theme 4: How should the performance of analysts be measured?

When asked about their view on how they believe an analyst's performance should be measured in order to address RQ6, 10 out of the 12 participants advocated for performance to be based on the quality of incident analysis and the associated report rather than quantitative metrics such as the number of incidents raised or closed. P2, a SOC manager in the defence sector, stated, *"I would certainly not measure analysts based on the number of tickets they raise. I would go for quality, not quantity, but I would be suspicious about someone who doesn't raise anything; I would wonder what we are paying them for."* This is an intriguing statement because, on the one hand, the manager does not want to use numbers as a measure, but they do want to know if someone is not raising any incidents.

P3 also suggested that the quality of an analyst's incident analysis be used to assess their performance. P3 commented, *"it comes back to quality checks on the analysis performed by an analyst. A step-by-step check. That is the only way you can measure the performance of an analyst."* P8 also expressed a similar viewpoint. P8 stated, *"quality of analysis to me is the most important thing. It's no good if someone is working on twenty incidents a day, of which none of them is particularly good quality."* Likewise, P7 articulated, *"I will measure the quality of the analysis based on the report, primarily because that is where you express your thought process. I cannot jump into another analyst's head, and in that sense, the report should be a reflection of their thinking. The quality of the analysis will be reflected in the quality of your report because it is your report that tells us your thoughts."*

P6 believed that it is difficult to measure an analyst's performance but suggested that *"the most important thing about any measure must come down to the quality of their work. The quality of the work outweighs the quantity."* P10 suggested that rather than just the output of what they are doing, they should be measured on the quality of their analysis: *"I think analysts should be measured on the quality of their analysis."* The consensus

amongst participants regarding measuring analysts based on the quality of their analysis reflects the fact that this is the area that takes up most of an analyst's time.

Even though the consensus among the participants was for the evaluation of an analyst's performance to be based on the quality of their analysis, some participants explained that cardinal numbers based on the number of times an analyst performs an activity should not be disregarded (P6, P11). However, participants recommended that there is a need to differentiate the priorities of the alerts or activities being dealt with by the analysts. P10 explained that analysts can be assessed based on the number of alerts that they detect, close and how they are dealt with - whether they have dealt with critical ones, high ones, medium ones or low ones. These classification and severity levels are also reported in the literature [35, 71, 72]. Also, P10 mentioned that an analyst's performance could be based on the number of use cases amended and the number of use cases created under the policy management function. P11 also suggested that when measuring an analyst's performance, consideration needs to be given to the number of false positives that the analyst has actioned. This position is also supported by P10, who advocates for false positives to be taken into consideration. Another suggestion by one of the participants was to use a weighted approach (P7); weights could be assigned to analysts' tasks in a SOC and then used to measure their performance.

Despite the strong agreement between SOC managers and analysts for analysts' performance to be based on the quality of incident analysis and quality of incident report, P12, a cyber incident director and head of security operations, stated, *"the issue with the quality check is that it is time-consuming, particularly if the SOC is a busy SOC and they have multiple tickets, and you've got a day job."*

Participants described what they considered to be a good analysis and listed a number of indicators that an analyst must look out for to achieve a *"good quality analysis."*

Given the strong preference from the participants to measure analysts based on the quality of their incident analysis and the quality of their reports, the literature was searched to ascertain whether there is existing work that addressed how to evaluate

analysts' performance based on the quality of their analysis and the quality of their incident reports. The section below presents the findings on the quality of the analysis and the quality report.

6.4 Guidelines for Assessing Quality of Incident Analysis and Report

One cannot play chess without knowing the rules.

Ben-Asher and Gonzalez [40]

The problem with evaluating performance based on the quality of analysis and the quality of an incident report is that the term "quality" is subjective. The definition of "quality" will differ from one person to the next [55]. Such activity cannot be measured unless it is properly defined [41]. This study proposes a guideline that can be used to assess the quality of an incident analysis. Establishing guidelines for assessing the quality of incident analysis and the quality of their report will enable both SOC managers and analysts to have a common agreement on what constitutes a quality analysis and report.

According to Alharbi [43], the overarching aim of an analyst when conducting an analysis is to ascertain whether it is a malicious activity and report it as a false positive or true positive. If it is a false positive, an analyst would typically recommend action such as tuning the signature out or amending it to improve the detection [199]. This viewpoint is supported by Feng et al. [42], who posit that analysts investigate an alert to decide if it is a genuine incident (true positive) or not (false positive). Similarly, Crémilleux et al. [97] state that an analysis of a security event should result in a determination of whether it is a true incident or a false positive.

Even though security researchers have suggested several questions that analysts should

consider when analysing security incidents, these studies fall short of providing a formal guideline that SOC managers and analysts can use to determine the quality of analysis and associated incident report [71, 76, 179]. For example, both Mutemwa et al. [71] and Miloslavskaya [218] emphasise the importance of an analyst's analysis addressing the *"who", "where", "when", "what", "why", and "how"* - (5W1H). Miloslavskaya [76] states that quality analysis ought to answer fundamental questions relating to: *who* the malicious person is (sources of alert); *what* actions have been taken; *where* the attacks originate from; and *when* the incident was identified, which relates to timestamp questions. Sundaramurthy et al. [179] also suggest similar criteria. Mutemwa et al. [71] mention the 5W1H but do not discuss in any detail what constitutes the 5W1H.

Using the insights gained from the interviews and suggestions from existing literature [71, 76, 179, 219, 220], the 5W1H was used to create a guideline that can be used to assess the analysis/report produced by analysts. The proposed guidelines (see Table 6.2) are intended to provide cues for analysts to aid them in their analysis and help others understand how they reached their conclusion in determining whether an alert is a false positive or true positive. Furthermore, this guideline will be useful to both experienced and novice analysts who, studies suggest, struggle with the complexities of security incident analysis tasks [2].

The proposed guidelines (See Table 6.2) was presented to a Delphi panel of SOC experts to solicit their opinion on the guidelines and also to elicit their view on additional cues in order to improve it. The results of the Delphi study, as well as the final guidelines, are presented in Section 6.5.4 in Table 6.13.

Table 6.2: Initial Proposed Guidelines for Assessing the Quality of Incident Analysis and Incident Report.

AN ANALYST NEEDS TO IDENTIFY & REPORT ON THE FOLLOWING ELEMENTS (IF AVAILABLE) TO ACHIEVE QUALITY ANALYSIS & QUALITY REPORT						
01 - WHO	02 - WHERE	03 - WHEN	04 - WHAT	05 - WHY	06 - HOW	07 - RECOMMENDATION
Who are the potential attackers/adversaries?	Where is the attacker or adversary targeting or likely to target and exploit?	When was the attack or incident first noticed?	What does the attacker already know? What capability do the attacker have?	Why is this incident of interest ?	How was the potential attack discovered?	Recommendation for addressing the incident.
• Attack Path (External threat or Insiders ?) • Source IP Address/Attacker IP Address • Source Port/Service • Source MAC Address • Attacker User Name • Attacker Host Name	• Impacted Host/Application • Destination IP Address/ Attacker IP Address • Destination Port/Service • Destination MAC Address • Location of Detection	• Date and Time of Detection • Reporting Device • Detection time Manager Receipt Time	• Name of Alert/Incident/Trigger • File/Email/URL Domain Name • Asset Name • User Account • IPS Signature/Use Case • Event ID/Type/OS • Breach Type • Incident Severity/Classification • File Hash • Indicator of Compromise	• Risk • Context -Geo Information and threat description	• Method of Detection • Mitigation Factors • Playbook used (Enter playbook used for incident, if any(Phishing Playbook, Enrichment Playbook etc)	• Containment Strategy • Mitigation Strategy • Any contact details (E.g. Email, Phone number, Office) - for further investigation Creation of a new use case or signature (if required)

6.5 Iteration 3 - Development of the SOC-AAM

6.5.1 Applying a decision-making model to devise a new evaluation method

The SOC-AAF developed in iteration 2 of the DSR process was used to develop the SOC-AAM, which offers a systematic approach for measuring the performance of an analyst. The SOC-AAF, as discussed in Section 6.3, consists of the main functions of an analyst and metrics for assessing their performance based on the findings from this study. The SOC-AAM uses the functions and metrics presented by the SOC-AAF and applies the AHP framework to assign weights to the functions of an analyst. The weights are then used as the basis to measure the performance of an analyst.

In order to build the SOC-AAM, the Delphi method was used alongside the AHP to get SOC experts to assign priorities (weights) to the functions expected of an analyst as presented in the SOC-AAF. The Delphi method was also used to solicit the opinions of the experts on the indicators that can be used to assess the quality of an analyst's incident analysis and the quality of their incident report. As reported in Chapter 3, the Delphi technique uses multiple rounds of expert engagement to reach consensus on a subject. Two rounds of the Delphi were applied in this study.

6.5.2 Round 1 of the Delphi-AHP Process

During Round 1 of the Delphi-AHP exercise, participants were given a questionnaire for the pairwise comparison exercise. The idea of the pairwise comparison was to compare two functions at a time on the basis of their relative importance in order to assign weight to them. This process is discussed in detail in the sections below. The questionnaire was created using a spreadsheet and distributed through email to the Delphi research participants, an approach similar to that suggested by Gordon [151].

The questionnaire also contained a table detailing some indicators for assessing the quality of incident analysis and incident report. The participants were requested to provide feedback on the indicators and to provide further suggestions. A copy of the questionnaire (AHP template) used for the Delphi study and the instructions for the panel on how to complete the template are stored in the links below:

https://git.cardiff.ac.uk/c1854157/delphi-exercise-the-ahp-template.git

https://git.cardiff.ac.uk/c1854157/delphi-exercise-instructions-for-completing-the-ahp-template.git

Table 6.3 shows the panel of experts that participated in this study. An invitation to recruit SOC experts to participate in the Delphi study was sent to all the participants that took part in the interviews, as well as analysts that were referred to the researchers by those experts that had already expressed interest. Among the twelve interview participants (see 6.1, only four responded and agreed to participate in the Delphi study. Those who could not participate cited busy schedules and workloads. An additional four SOC experts who did not participate in the interviews agreed to participate in the Delphi study, resulting in a total of eight participants.

Table 6.3: Delphi Panel Participants' Profile and Organisation

Delphi Panel	Job Title	Industry
Participant 1	Senior Analyst	Defence Sector
Participant 2	Senior Analyst/Consultant	Finance Sector
Participant 3	SOC Analyst	Airline
Participant 4	Cyber Operations Specialist	Telecom
Participant 5	SOC Consultant	Defence Sector
Participant 6	Cyber Incident Director and Deputy Head of Security Operations	Automobile
Participant 7	SOC Manager	Finance Sector (Professional Services)
Participant 8	Analyst	Defence Sector

The AHP technique adopted in this study for establishing the weights for the different functions is similar to the approach suggested by Islam and bin Mohd Rasad [60]. In [60], the authors outlined four steps under the AHP that could be used to evaluate the performance of employees using the AHP framework. These steps are:

i Identify the criteria, subcriteria and employees to be evaluated and construct the AHP model/hierarchy;

ii Construct an $n \times n$ pairwise comparison matrix for the criteria.

Calculate the weights of the decision criteria by computing the normalised principal eigenvector of the matrix [221]. This vector gives the weights of the criteria [60, 222, 223]. Construct a pairwise comparison for the subcriteria and calculate the weights in a similar manner. The weights of the subcriteria are multiplied by their respective parent criterion;

iii Divide each subcriterion into intensities or grades, such as high, medium, and low. The intensity allows one to determine the quality of an alternative for that criterion [68]. Priorities are assigned to the intensities by conducting a pairwise comparison. The priorities of the intensities are multiplied by the weight of their parent subcriterion;

iv Finally, take each employee and measure their performance intensity under each subcriterion, then add the global priorities of the intensities for the employee. Repeat the process for all the employees.

In this research, step (iii) is replaced with the inherent intensities of the metrics: the individual metrics achieved by an analyst under step (ii) are also used as the distinguishing factor rather than creating a new set of intensities [69]. As explained by Saaty [68, p.136], the purpose of intensities is to distinguish the quality of an alternative for that criterion. Since most of the metrics under the subcriteria (see Figure 6.3) are already serving as a distinguishing factor (for example, incidents processed by analysts are categorised as high incidents, medium incidents and low incidents [35, 72]), this study contends that there is no need for additional intensities to be created. Also, no intensities are created under the intelligence function, the policies and signatures management function, and the baseline and vulnerability management function because the metrics under these functions are deemed sufficient to capture the performance of an analyst,

based on the findings from the engagement with SOC experts [55]. This strategy is similar to the work of Vargas [222], who did not use intensities. In step (iv), each analyst is measured against each metric, and the total of the metrics is used to determine their overall score.

6.5.2.1 A Hierarchical Model for Measuring the Performance of an Analyst

A hierarchical model shown in Figure 6.3 was constructed and used as the foundation for devising an assessment method for analysts. Creating a hierarchy simplifies the problem and aids in the identification of criteria and subcriteria to be used. The functions are represented as the criteria and the metrics or KPIs as the subcriteria.

1. The first level of the hierarchy represents the goal or focus of the problem, as shown in Figure 6.3. The goal in this research is to measure the overall performance of an analyst.

2. The second level of the hierarchy represents the criteria needed for the evaluation process - Figure 6.3. In this study, the criteria are the functions expected of the analyst deduced from the empirical interview data collected from SOC experts and a thorough analysis of existing literature [21, 30, 52, 147].

3. The third level of the hierarchy represents the subcriteria for each respective main criteria - Figure 6.3. In this research, the metrics associated with each of the functions are used as the subcriteria.

4. The final level represents the analysts who are evaluated one at a time with the criteria and subcriteria defined above. The word *"alternatives"* is often used in the AHP hierarchy to denote the final level [168].

As a part of the Delphi-AHP exercise, the participants were requested to conduct a pairwise comparison exercise using the AHP framework in order to assign weights

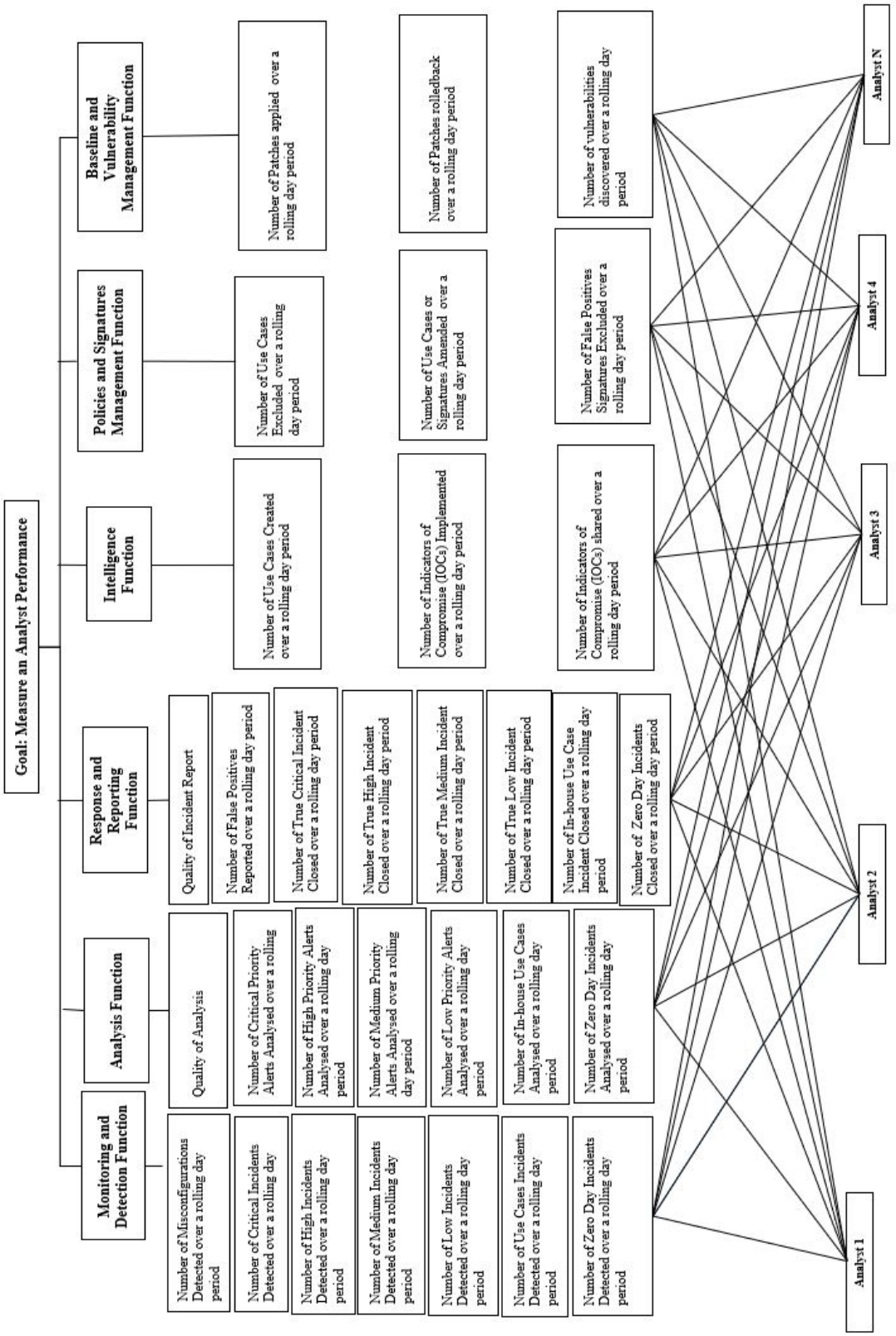

Figure 6.3: SOC Analysts' Assessment Criteria and Subcriteria

to the functions. A pairwise comparison matrix A was constructed and given to the participants. The comparison matrix was subsequently used to compute the weights for the criteria and subcriteria. The matrix A is an $n \times n$ real matrix, where n is the number of evaluation criteria or subcriteria being considered. Let a_{ij} be a pairwise comparison that the decision-maker makes between two criteria i and j. Each entry a_{ij} of the matrix A represents the importance of the ith criterion relative to the jth criterion. Note that, a_{ij} denotes the entry in the ith row and the jth column of matrix A. If $a_{ij} > 1$, then the ith criterion is more important than the jth criterion, whereas if $a_{ij} < 1$, then the ith criterion is less important than the jth criterion. If the two criteria have the same importance, then the entry a_{ij} will be equal to 1 [68]. In AHP, the entries a_{ij} and a_{ji} satisfy the constraint: $a_{ij} \cdot a_{ji} = 1$ and $a_{ii} = 1$ for all i because when you compare a criterion against itself, the expected outcome is of equal importance. If $a_{ij} = 1$, it means that the decision-maker regards element i and j as equally important.

The participants rated the relative importance between two criterion at a time. This was done using a numerical scale ranging from 1 to 9, shown in Table 6.4 as proposed by Saaty [68]. When $a_{ij} = 3, 5, 7$ and 9 the decision-maker(s) regards element i as being moderately more important, strongly more important, very strongly more important, and extremely important, respectively, to element j. Saaty [68] suggests that an intermediate value $(2, 4, 6, 8)$ can be used if the decision-maker seeks to compromise.

Table 6.4: Saaty's Scale of Relative Importance [68]

AHP Comparison Scale (a_{ij})	Numerical Rating	Meaning
Extremely Important	9	*i* is extremely more important than *j*
Very Strong to Extremely Important	8	
Very Strongly Important	7	*i* is strongly more important than *j*
Strongly to very Strongly Important	6	
Strongly Important	5	*i* is more important than *j*
Moderately to Strongly Important	4	
Moderately to Important	3	*i* is moderately more important than *j*
Equally to moderately	2	
Equally Important	1	*i* and *j* are equally important

Once the matrix A has been constructed, the priority vector (or weights) for the criteria [60, 161] was computed. The strategy for calculating the weights starts by deriving from the matrix A a normalised pairwise comparison matrix (A_{norm}) by making the

sum of each column equal to 1 [221]. Equation 6.1 is used for the computation. Each entry $\overline{a}_{ij}$ of the matrix A_{norm} is computed, using Equation 6.1.

$$\overline{a}_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \tag{6.1}$$

Finally, the criteria weight vector (w) is calculated by averaging the entries on each row of A_{norm} using Equation 6.2 [221, 224].

$$w_i = \frac{\sum_{j=1}^{n} \overline{a}_{ij}}{n} \tag{6.2}$$

6.5.2.2 Checking the Consistency of the Decision Matrices

A consistency check is performed to ensure that the values assigned in the comparison matrix and the resultant weights or priorities were not done arbitrarily [68, 221]. The AHP provides a technique for checking the consistency of the choices made by the decision-maker [172]. The concept of a consistency check is straightforward. If one prefers *summer* twice as much as *spring* and *spring* twice as much as *winter*, in mathematical terms, the preference of *summer* to *winter* would be 4. If the decision-maker assigns any other value, there would be a certain level of inconsistency in the judgement [68]. However, Saaty acknowledges that since the judgements are made using subjective preferences, it is unlikely one can completely avoid some level of inconsistency. The AHP, therefore, allows for a certain level of inconsistency in the judgement.

The AHP calculates the consistency ratio (CR) to ascertain whether the judgements made are at an acceptable level of consistency. The (CR) is calculated by comparing the consistency index (CI) of the matrix A versus the consistency index of a randomly

generated matrix - Random Index (RI). (CR) can be calculated using Equation 6.3 [68].

$$CR = \frac{CI}{RI} \tag{6.3}$$

In Equation 6.3, RI denotes a Random Index. RI is when the values are entered randomly without any thought process. If the values are randomly assigned, one would expect it to be inconsistent [68]. Table 6.5 shows the values for RI [68].

Also, the CI in Equation 6.3 is calculated using Equation 6.4, where (λ_{max}) represents the maximum eigenvalue of the decision matrix A and n is the number of compared criteria [68]. If A is absolutely consistent, then $\lambda_{max} = n$ [222].

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{6.4}$$

Table 6.5: Consistency indices for a randomly generated matrix

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.52	1.54	1.56	1.58	1.59

It is generally accepted that if the consistency ratio CR of the decision matrix is less than 10%, then the judgement is acceptable and can therefore be used [161].

After calculating the main criteria, a similar calculation is performed for all of the subcriteria to determine local priorities (subcriteria weights). Once the local priorities of the elements of the various subcriteria have been calculated, they can be aggregated to obtain the final weights [222].

6.5.3 Analysing the Output from Round 1

The response from each participant regarding the AHP pairwise comparison was checked to ascertain whether their values and results satisfied the rule of reciprocity and were

also aligned to the AHP consistency index [225]. The rule of reciprocity dictates that if criteria A is more important than B, then B has to be less important than A. The output for all eight participants for each of the criteria and subcriteria was consistent and had CI of $< 10\%$. The results of each participant are shown in Appendix D to J.

The geometric mean values were calculated using the responses of all participants. The geometric mean values were then used to create a comparison matrix for the group [68]. The consistency index of the group's decision was then checked to ascertain whether the group's judgment was consistent and met the AHP acceptable standards. Given that a questionnaire was used to solicit the opinion of experts regarding the weights that should be assigned to the different functions and metrics, the researcher was mindful of the possibility of not obtaining a group consensus consistent with the AHP standard given differences in opinion. Saaty [68, p. 270] mentions that when questionnaires are used, there are times when the outcome from the group may be inconsistent, yet it "provides an overall representation of the judgement of the group."

6.5.3.1 Decision Matrix for the Main Criteria

Figure 6.4 illustrates the main criteria for evaluating an analyst's performance. A pairwise comparison matrix was constructed to derive the weights criteria for evaluating an analyst's performance. The pairwise comparison matrix from each of the participants is shown in Appendix D. The analysis of the data from the panel in Round 1 shows a consensus from the group that is consistent with the AHP standard of $< 10\%$. The resultant weights for each of the functions are shown in Table 6.6, along with the CR.

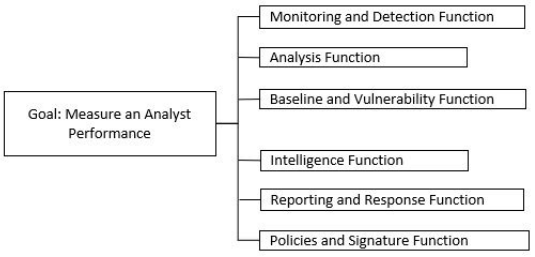

Figure 6.4: Main Criteria

Table 6.6: Pairwise Comparison Matrix for the Main Criteria, Weights and CR

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function	Criteria Weights
Monitoring and Detection Function	1	1	3	3	1	2	0.2494
Analysis Function	1	1	3	2	1	3	0.2450
Baseline and Vulnerability Function	1/3	1/3	1	1	1	1	0.1084
Intelligence Function	1/3	1/2	1	1	1	2	0.1302
Response and Reporting Function	1	1	1	1	1	2	0.1769
Policies and Signature Function	1/2	1/3	1	1/2	1/2	1	0.0901
						CR =	0.0327

The weights for the subcriteria were determined in the same way that the weights for the main criteria were determined: by computing the geometric mean of the pairwise values suggested by each participant and constructing a comparison matrix, as described above. For each comparison matrix, the CR was also calculated to ascertain the consistency of the judgement.

6.5.3.2 Decision Matrix for the Monitoring and Detection Function Subcriteria

The subcriteria for the monitoring and detection function are depicted in Figure 6.5. A pairwise comparison matrix was constructed for the monitoring and detection function criteria, as shown in Table 6.7, using the criteria metrics. The resultant weights for criteria based on the group's judgement are deduced along with the consistency index as shown in Table 6.7. The individual responses from the participants are shown in Appendix E.

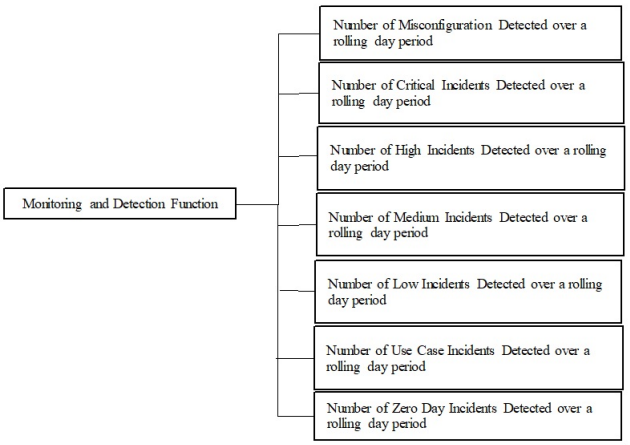

Figure 6.5: Monitoring and Detection Function Criteria

Table 6.7: Weights and Consistency Ratio (CR) for the Monitoring and Detection Function Subcriteria.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period	Subcriteria Weights
Number of Misconfiguration Detected over a rolling period	1	1/5	1/3	1/2	1	1/2	1/5	0.0507
Number of Critical Incidents Detected over a rolling period	5	1	2	2	5	1	1/2	0.2001
Number of High Incidents Detected over a rolling period	3	1/2	1	2	4	1	1/3	0.1390
Number of Medium Incidents Detected over a rolling period	2	1/2	1/2	1	3	1	1/5	0.0972
Number of Low Incidents Detected over a rolling period	1	1/5	1/4	1/3	1	1/3	1/5	0.0442
Number of Use Case Incidents Detected over a rolling period	2	1	1	1	3	1	1/3	0.1262
Number of Zero Day Incidents Detected over a rolling period	5	2	3	5	5	3	1	0.3427
							CR =	0.0235

6.5.3.3 Decision Comparison Matrix for the Analysis Function Subcriteria

The criteria shown in Figure 6.6 were used by the experts to construct a pairwise comparison. Individual responses from the participants are shown in Appendix F. The results of aggregating the geometric mean values and using them to build the group comparison matrix generated the weights and the consistency index are shown in Table 6.8.

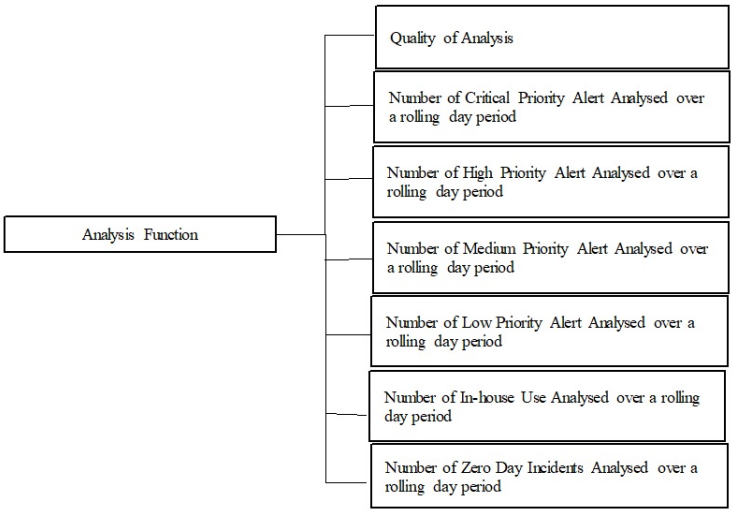

Figure 6.6: Analysis Function Criteria

Table 6.8: Weights and Consistency Ratio (CR) for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period	Subcriteria Weights
Quality of Analysis	1	5	6	6	6	5	4	0.4427
Number of Critical Priority Alert Analysed over a rolling period	1/5	1	1	2	3	1	1	0.1091
Number of High Priority Alert Analysed over a rolling period	1/6	1	1	2	3	1	1/2	0.0974
Number of Medium Priority Alert Analysed over a rolling period	1/6	1/2	1/2	1	2	1	1/4	0.0640
Number of Low Priority Alert Analysed over a rolling period	1/6	1/3	1/3	1/2	1	1/3	1/3	0.0416
Number of In-house Use case Analysed over a rolling period	1/5	1	1	1	3	1	1/2	0.0910
Number of Zero Day Incidents Analysed over a day rolling period	1/4	1	2	4	3	2	1	0.1544
							CR =	0.0293

6.5.3.4 Decision Comparison Matrix for the Response and Reporting Function Subcriteria

Figure 6.7 illustrates the subcriteria for the Response and Reporting function. Again, as with the previous subcriteria, a pairwise comparison matrix was constructed for the

Response and Reporting function criteria, as shown in Table 6.9 using the geometric mean values from individual values provided by the experts. The individual responses are shown in Appendix G. Table 6.9 shows the resulting weights and the consistency index based on the group's judgement.

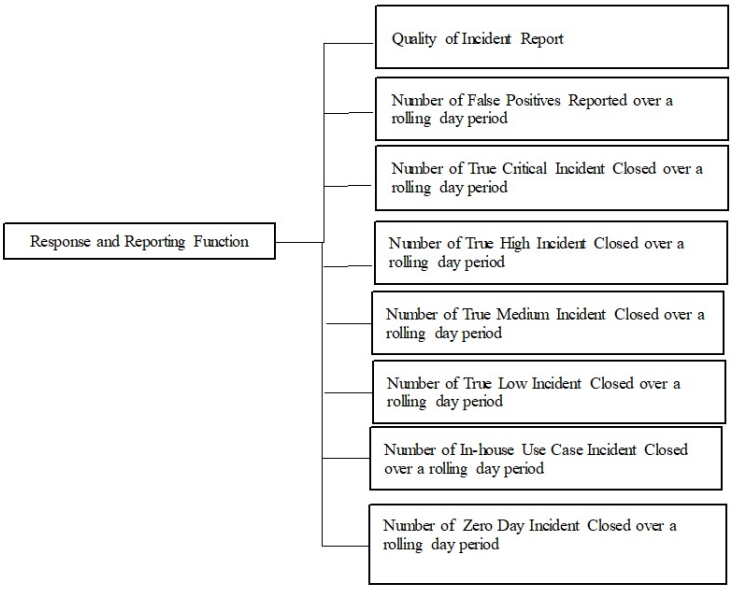

Figure 6.7: Response and Reporting Function Criteria

Table 6.9: Weights and Consistency Ratio (CR) for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period	Subcriteria Weights
Quality of Incident Report	1	5	5	5	5	5	4	3	0.3641
Number of False Positives Reported over a rolling period	1/5	1	1/3	1/3	1	1	1/2	1/5	0.0468
Number of True Critical Incident Closed over a rolling period	1/5	3	1	1	2	2	1	1	0.1090
Number of True High Incident Closed over a rolling period	1/5	3	1	1	2	2	1	1/2	0.0995
Number of True Medium Incident Closed over a rolling period	1/5	1	1/2	1/2	1	2	1	1/3	0.0648
Number of True Low Incident Closed over a rolling period	1/5	1	1/2	1/2	1/2	1	1	1/5	0.0516
Number of In-house Use Case Incidents Closed over a rolling period	1/4	2	1	1	1	1	1	1/3	0.0781
Number of Zero Day Closed over a rolling period	1/3	5	1	2	3	5	3	1	0.1862
								CR =	0.0299

6.5.3.5 Decision Comparison Matrix for the Intelligence Function Subcriteria

Figure 6.8 depicts the subcriteria for the intelligence function. A pairwise comparison matrix was constructed using the geometric mean of the individual pairwise comparison values provided by the experts. The individual responses are shown in Appendix H. The resultant weights and the consistency index from the group's judgement are shown in Table 6.10.

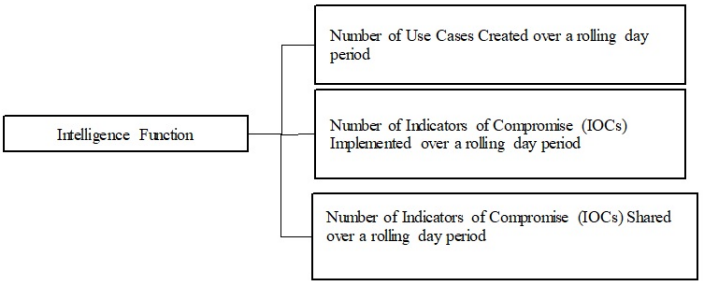

Figure 6.8: Intelligence Function Criteria

Table 6.10: Weights and Consistency Ratio (CR) for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented	Number of Indicators of Compromised (IOCs) Shared over	Subcriteria Weights
Number of Use Cases Created over a rolling period	1	1	2	0.3873
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	3	0.4429
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/2	1/3	1	0.1698
			CR =	0.0158

6.5.3.6 Decision Comparison Matrix for the Baseline and Vulnerability Function Subcriteria

Figure 6.9 illustrates the subcriteria for the Baseline and Vulnerability function. A pairwise comparison matrix was constructed for the Baseline and Vulnerability function criteria using the geometric mean values from the individual expert judgement. Table 6.11 shows the resulting weights and the consistency index.

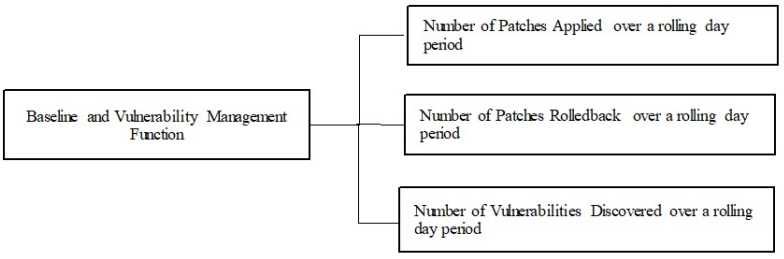

Figure 6.9: Baseline and Vulnerability Function Criteria

Table 6.11: Weights and Consistency Ratio (CR) for the Baseline and Vulnerability Management Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period	Subcriteria Weights
Number of Patches Applied over a rolling period	1	2	1	0.3873
Number of Patches Rolled back over a rolling period	1/2	1	1/3	0.1698
Number of Vulnerabilities Discovered over a rolling period	1	3	1	0.4429
			CR =	0.0158

6.5.3.7 Decision Comparison Matrix for the Policies and Signature Management Subcriteria

The subcriteria for the Policies and Signatures Management function is depicted in Figure 6.10. A pairwise comparison matrix was constructed for the policies and signature management function subcriteria using the geometric mean values provided by each expert. Individual responses are shown in Appendix I. The resultant weights and the consistency index are shown in Table 6.12.

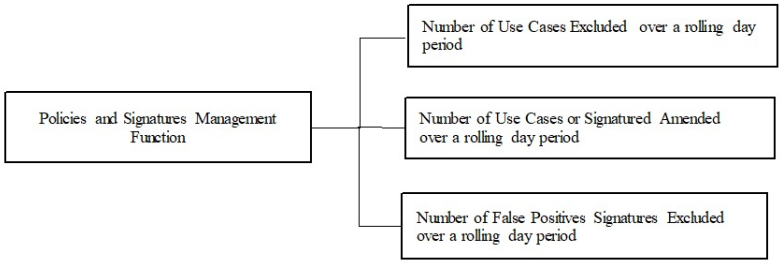

Figure 6.10: Policies and Signature Management Function Criteria

Table 6.12: Weights and Consistency Ratio (CR) for the Policies and Signature Management Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period	Subcriteria Weights
Number of Use Cases Excluded over a rolling period	1	1/2	1	0.2500
Number of Use Cases or Signatures Amended over a rolling period	2	1	2	0.5000
Number of False Positives Signatures Excluded over a rolling period	1	1/2	1	0.2500
			CR =	0.00

In addition to the weights, the indicators for assessing the quality of incident analysis and the quality of their report were also established. Following the two rounds of the Delphi study, the indicators identified in Table 6.13 were reported by the participants as the most important areas that must be reported by analysts as part of quality analysis and in their reports. These indicators can help assess the quality of an incident report written by an analyst.

Table 6.13: Quality of Analysis and Quality Report Indicators

AN ANALYST NEEDS TO IDENTIFY & REPORT ON THE FOLLOWING INDICATORS (IF AVAILABLE) TO ACHIEVE QUALITY ANALYSIS & QUALITY REPORT						
01 - WHO	02 - WHERE	03 - WHEN	04 - WHAT	05 - WHY	06 - HOW	07 - RECOMMENDATION
Who are the potential attackers/adversaries?	Where is the attacker or adversary targeting or likely to target and exploit?	When was the attack or incident first noticed?	What does the attacker already know? What capability do the attacker have?	Why is this incident of interest ?	How was the potential attack discovered?	Recommendation for addressing the Incident.
• Attack Path (External threat or Insiders ?) • Source IP Address/Attacker IP Address • Source Port/Service • Source MAC Address • Attacker Username (if internal) • Attacker Host Name • Attacker User Agent (if applicable) •Is the source IP information known? •Is the destination IP information known? • Is the source Port information known? • Is the source Port information known? • Is the username of the attacker known?	• Impacted Host/Application • Destination IP Address/ Attacker IP Address • Destination Port/Service • Destination MAC Address • Location of Detection • Has network or client machine involved been identified? • Did the event occur in the DMZ? • Has the log sources been identified? • Has the source of the event been identified?	• Date and Time of Detection including time zone • Reporting Device • Detection time •Manager Receipt Time • Is the event still continuing?	• Name of Alert/Incident/Trigger • File/Email/URL Domain Name • Asset Name • User Account • IPS Signature/Use Case • Event ID/Type/OS • Breach Type • Incident Severity/Classification • File Hash • Indicator of Compromise •Vulnerabilities of the target system (with or without public exploits) •Is offence about reconnaissance? • Is offence about attack delivery? • Is offence about exploitation? • Is offence about system compromise?	• Risk • Context and geographical Information and threat description • System criticality • Potential Impact • Has the rules associated with the incident been identified? • Has the first rule that triggered the incident been identified? • Was the rule updated recently? • Was there any rules testing in place?	• Method of Detection • Mitigation Factors • Playbook used (Enter playbook used for incident, if any(Phishing Playbook, Enrichment Playbook etc) • Did the attacker download any executable? • Is it a known attacker? • Did the attacker access malicious website? • Does the computer have any vulnerability?	•Containment Strategy • Mitigation Strategy • Any contact details (E.g. Email, Phone number, Office) - for further investigation •Creation of a new use case or signature (if required) • Eradication and remediation • Return to business operations

6.5.4 Round 2 of the Delphi-AHP study and Final Ranking

The purpose of Round 2 was to see if the experts agreed with the group consensus reached in Round 1 or if any participants wanted to change some of the values derived from the group judgement. Furthermore, Round 2 allowed the experts to make any changes to the criteria weights or to recommend comments on the criteria for assessing the quality of the analysis and incident report.

The outcome of Round 2 revealed some interesting results in that none of the participants changed the outcome of the first round. The weights for the criteria and subcriteria from the two rounds were synthesised to produce a set of overall weights (also known as the "global weights") by multiplying the weight of each criterion by the weights of their respective subcriterion [222]. The output of the calculation is shown in Table 6.14.

Table 6.14: Final Weights for Analysts' Functions and Metrics/KPIs

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×)their respective sub-criterion weight**	**Global Weights(×)100**
Monitoring and Detection Function	0.2494			
Number of Misconfiguration Detected over a rolling period		0.0507	0.0126	1.2640
Number of Critical Incidents Detected over a rolling period		0.2001	0.0499	4.9901
Number of High Incidents Detected over a rolling period		0.1390	0.0347	3.4677
Number of Medium Incidents Detected over a rolling period		0.0972	0.0242	2.4249

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Number of Low Incidents Detected over a rolling period		0.0442	0.0110	1.1013
Number of Use Case Incidents Detected over a rolling period		0.1262	0.0315	3.1470
Number of Zero Day Incidents Detected over a rolling period		0.3427	0.0855	8.5479
Analysis Function	0.2450			
Quality of Analysis		0.4427	0.1084	10.8440
Number of Critical Priority Alert Analysed over a rolling period		0.1091	0.0267	2.6716

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Number of High Priority Alert Analysed over a rolling period		0.0974	0.0239	2.3866
Number of Medium Priority Alert Analysed over a rolling period		0.0640	0.0157	1.5667
Number of Low Priority Alert Analysed over a rolling period		0.0416	0.0102	1.0180
Number of In-house Use case Analysed over a rolling period		0.0910	0.0223	2.2288

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion($\times$) their respective subcriterion weight**	**Global Weights($\times$)100**
Number of Zero Day Incidents Analysed over a day rolling period		0.1544	0.0378	3.7817
Baseline and Vulnerability Function	0.1084			
Number of Patches Applied over a rolling period		0.3873	0.0420	4.1982
Number of Patches Rolled back over a rolling period		0.1698	0.0184	1.8410
Number of Vulnerabilities Discovered over a rolling period		0.4429	0.0480	4.8004

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Intelligence Function	0.1302			
Number of Use Cases Created over a rolling period		0.3873	0.0504	5.0432
Number of Indicators of Compromised (IOCs) implemented over a rolling period		0.4429	0.0577	5.7666
Number of Indicators of Compromised (IOCs) shared over a rolling period		0.1698	0.0221	2.2116
Response and Reporting Function	0.1769			

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Quality of Incident Report		0.3641	0.0644	6.4403
Number of False Positives Reported over a rolling period		0.0468	0.0083	0.8276
Number of True Critical Incident Closed over a rolling period		0.1090	0.0193	1.9277
Number of True High Incident Closed over a rolling period		0.0995	0.0176	1.7594
Number of True Medium Incident Closed over a rolling period		0.0648	0.0115	1.1455

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Number of True Low Incident Closed over a rolling period		0.0516	0.0091	0.9129
Number of In-house Use Case Incidents Closed over a rolling period		0.0781	0.0138	1.3817
Number of Zero Day Closed over a rolling period		0.1862	0.0329	3.2930
Policies and Signature Function	0.0901			
Number of Use Cases Created over a rolling period		0.2500	0.0225	2.2527

Table 6.14 – continued from previous page

Criteria and Subcriteria	**Criteria Weights**	**Subcriteria Weights**	**Global weight = the weight of each criterion(×) their respective subcriterion weight**	**Global Weights(×)100**
Number of Indicators of Compromised (IOCs) implemented over a rolling period		0.5000	0.0451	4.5053
Number of Indicators of Compromised (IOCs) shared over a rolling period		0.2500	0.0225	2.2527
Total Weight			1	100

6.6 SOC-AAM Template

The weights presented in Table 6.14 are used in this research to create the SOC-AAM (Table 6.15). The SOC-AAM was tested and evaluated as part of an experimental case study in Chapter 7. The performance score for one of the analyst's that participated in this study is shown in Table 6.16 and used to illustrate the composition of the SOC-AAM. All the performance scores from the experimental case study can be found by following the link below:

https://git.cardiff.ac.uk/c1854157/analysts-performance-scores.git

Table 6.15: SOC-AAM: Assessment Template

ASSESSMENT CRITERIA AND SUBCRITERIA (Cij)	WEIGHTS (W_{ij})	AN ANALYST'S KPI SCORE (*As a value or cardinal number based on the number of times a subcriterion task is performed by an analyst) (M_{ij})	AN ANALYST'S TOTAL SCORE PER EACH SUBCRITERION ($S=W_{ij}*M_{ij}$)	THE TEAM'S KPI SCORE FOR EACH SUBCRITERION (*As a value or cardinal number based on the number of times a subcriterion task is performed by the team) (T_{ij})	THE TEAM'S TOTAL SCORE FOR EACH SUBCRITERION ($O=W_{ij}*T_{ij}$)
Monitoring and Detection Function					
Number of Misconfiguration Detected over a rolling period	1.2640		0.0000		0.0000
Number of Critical Incidents Detected over a rolling period	4.9901		0.0000		0.0000
Number of High Incidents Detected over a rolling period	3.4677		0.0000		0.0000
Number of Medium Incidents Detected over a rolling period	2.4249		0.0000		0.0000
Number of Low Incidents Detected over a rolling period	1.1013		0.0000		0.0000
Number of Use Case Incidents Detected over a rolling period	3.1470		0.0000		0.0000
Number of Zero Day Incidents Detected over a rolling period	8.5479		0.0000		0.0000
Analysis Function					
Quality of Analysis	10.8440		0.0000		0.0000
Number of Critical Priority Alert Analysed over a rolling period	2.6716		0.0000		0.0000
Number of High Priority Alert Analysed over a rolling period	2.3866		0.0000		0.0000
Number of Medium Priority Alert Analysed over a rolling period	1.5667		0.0000		0.0000
Number of Low Priority Alert Analysed over a rolling period	1.0180		0.0000		0.0000
Number of In-house Use case Analysed over a rolling period	2.2288		0.0000		0.0000
Number of Zero Day Incidents Analysed over a day rolling period	3.7817		0.0000		0.0000
Baseline and Vulnerability Function					
Number of Patches Applied over a rolling period	4.1982		0.0000		0.0000
Number of Patches Rolled back over a rolling period	1.8410		0.0000		0.0000
Number of Vulnerabilities Discovered over a rolling period	4.8004		0.0000		0.0000
					0.0000
Intelligence Function					
Number of Use Cases Created over a rolling period	5.0432		0.0000		0.0000
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	5.7666		0.0000		0.0000
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2116		0.0000		0.0000
					0.0000
Response and Reporting Function					
Quality of Incident Report	6.4403		0.0000		0.0000
Number of False Positives Reported over a rolling period	0.8276		0.0000		0.0000
Number of True Critical Incident Closed over a rolling period	1.9277		0.0000		0.0000
Number of True High Incident Closed over a rolling period	1.7594		0.0000		0.0000
Number of True Medium Incident Closed over a rolling period	1.1455		0.0000		0.0000
Number of True Low Incident Closed over a rolling period	0.9129		0.0000		0.0000
Number of In-house Use Case Incidents Closed over a rolling period	1.3817		0.0000		0.0000
Number of Zero Day Closed over a rolling period	3.2930		0.0000		0.0000
Policies and Signature Function					
Number of Use Cases Excluded over a rolling period	2.2527		0.0000		0.0000
Number of Use Cases or Signatures Amended over a rolling period	4.5053		0.0000		0.0000
Number of False Positives Signatures Excluded over a rolling period	2.2527		0.0000		0.0000
Total Weights	100.0000		0.0000		0.0000
Analyst's Overall Performance (X)	0.0000				
Team's Overall Performance (Y)	0.0000				
Individual Analyst's Percentage Contribution (Z) %	#DIV/0!				
Team's Percentage Contribution (%)	#DIV/0!				

Table 6.16: Demonstration of the SOC-AAM

1. Criterion (i) Subcriterion (j)
2. Weight for a subcriterion (w_{ij})
3. A value or cardinal number achieved by an analyst for a subcriterion (m_{ij})
4. An analyst's total score for a subcriterion ($S=w_{ij}*m_{ij}$)
5. Team's score for a subcriterion (t_{ij})
6. Team's overall score for each subcriterion ($O=w_{ij}*t_{ij}$)

ASSESSMENT CRITERIA AND SUBCRITERIA (C_{ij})	WEIGHTS (W_{ij})	AN ANALYST'S KPI SCORE (*As a value or cardinal number based on the number of times a subcriterion task is performed by an analyst) (M_{ij})	AN ANALYST'S TOTAL SCORE PER EACH SUBCRITERION ($S=W_{ij}*M_{ij}$)	THE TEAM'S KPI SCORE FOR EACH SUBCRITERION (*As a value or cardinal number based on the number of times a subcriterion task is performed by the team) (T_{ij})	THE TEAM'S TOTAL SCORE FOR EACH SUBCRITERION ($O=W_{ij}*T_{ij}$)
Monitoring and Detection Function					
Number of Misconfiguration Detected over a rolling period	1.2640		0.0000		0.0000
Number of Critical Incidents Detected over a rolling period	4.9901		0.0000		0.0000
Number of High Incidents Detected over a rolling period	3.4677		0.0000	1	3.4677
Number of Medium Incidents Detected over a rolling period	2.4249		0.0000	58	140.6455
Number of Low Incidents Detected over a rolling period	1.1013	6	6.6077	64	70.4816
Number of Use Case Incidents Detected over a rolling period	3.1470		0.0000		0.0000
Number of Zero Day Incidents Detected over a rolling period	8.5479		0.0000		0.0000
Analysis Function					
Quality of Analysis	10.8440	7	75.9082	91	986.8068
Number of Critical Priority Alert Analysed over a rolling period	2.6716		0.0000		0.0000
Number of High Priority Alert Analysed over a rolling period	2.3866		0.0000	1	2.3866
Number of Medium Priority Alert Analysed over a rolling period	1.5667		0.0000	58	90.8665
Number of Low Priority Alert Analysed over a rolling period	1.0180	6	6.1077	64	65.1492
Number of In-house Use case Analysed over a rolling period	2.2288		0.0000		0.0000
Number of Zero Day Incidents Analysed over a day rolling period	3.7817		0.0000		0.0000
Baseline and Vulnerability Function					
Number of Patches Applied over a rolling period	4.1982		0.0000		0.0000
Number of Patches Rolled back over a rolling period	1.8410		0.0000		0.0000
Number of Vulnerabilities Discovered over a rolling period	4.8004		0.0000		0.0000
					0.0000
Intelligence Function					
Number of Use Cases Created over a rolling period	5.0432		0.0000		0.0000
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	5.7666		0.0000		0.0000
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2116		0.0000		0.0000
					0.0000
Response and Reporting Function					
Quality of Incident Report	6.4403	7	45.0820	91	586.0664
Number of False Positives Reported over a rolling period	0.8276		0.0000		0.0000
Number of True Critical Incident Closed over a rolling period	1.9277		0.0000		0.0000
Number of True High Incident Closed over a rolling period	1.7594		0.0000		0.0000
Number of True Medium Incident Closed over a rolling period	1.1455	7	8.0184	114	130.5855
Number of True Low Incident Closed over a rolling period	0.9129	2	1.8258	80	73.0322
Number of In-house Use Case Incidents Closed over a rolling period	1.3817		0.0000		0.0000
Number of Zero Day Closed over a rolling period	3.2930		0.0000		0.0000
Policies and Signature Function					
Number of Use Cases Excluded over a rolling period	2.2527		0.0000		0.0000
Number of Use Cases or Signatures Amended over a rolling period	4.5053		0.0000		0.0000
Number of False Positives Signatures Excluded over a rolling period	2.2527		0.0000		0.0000
Total Weights	100.0000		143.5499		2149.4880

Analyst's Overall Performance (X)	143.5499
Team's Overall Performance (Y)	2149.4880
Individual Analyst's Percentage Contribution (Z) %	6.6783
Team's Percentage Contribution (%)	100.0000

The SOC-AAM (Table 6.15) contains six **criteria** and 31 **subcriteria**. The terms criteria and subcriteria are used as a part of utilising the AHP framework [167, 226] in this study (see Figure 6.3). The criteria are the analysts' functions and the subcriteria are the KPIs/metrics for measuring their performance under each function as discussed in Section 6.5.2.1.

The weights for the **subcriteria** under the **criteria** are employed during the performance measurement. It is important to note that the criterion weight is simply the summation of the subcriteria weights for each criterion, respectively.

The steps to using the SOC-AAM as a performance measurement tool are detailed below. The process is facilitated by an Excel spreadsheet that automates all calculations. A copy of the SOC-AAM can be found here:

https://git.cardiff.ac.uk/c1854157/the-soc-aam.git

Below presents how the performance scores in the SOC-AAM is computed.

1. In the SOC-AAM (Table 6.16), let $C_{ij} = (c_{i1}, c_{i2}, c_{i3} \cdots, c_{ij})$; represent the **first column** of the Table; where i represents a criterion; $1 \leq i \leq 6$ (as there are six criteria in the SOC-AAM); j denotes a subcriterion under the ith criterion; $1 \leq j \leq N_i$ and N_i denotes the total number subcriteria for the ith criterion. For example, c_{11} represents the first subcriterion for the first criterion; c_{12} represents the second subcriterion for the first criterion, c_{13} represents the third subcriterion for the first criterion, and so on and so forth. In Table 6.16, the cells representing the criteria are colour-coded blue and those representing the subcriteria colour-coded in grey.

2. Let $W_{ij} = (w_{i1}, w_{i2}, w_{i3} \cdots, w_{ij})$ represent the **second column** of the SOC-AAM (Table 6.16); where w_{ij} represents the weight for the jth subcriterion of the ith criterion. The weights are deduced in Section 6.5.3 and presented in Table 6.14.

3. Let $M_{ij} = (m_{i1}, m_{i2}, m_{i3} \cdots, m_{ij})$ represent the **third column** of the SOC-AAM (Table 6.16); where m_{ij} represents a value or cardinal number [196] based on counting the number of times an analyst performs a task represented by the jth subcriterion of the ith criterion. For example, an analyst that has closed 2 medium incidents, would be assigned a value of 2 under the number of medium incidents closed.

4. In the **fourth column** (Table 6.16), an analyst's total score (S) for the jth subcriterion of the ith criterion is computed in as $S = w_{ij} \times m_{ij}$.

5. The **fifth column** (Table 6.16) represents the team's scores for each subcriterion. Let $T_{ij} = (t_{i1}, t_{i2}, t_{i3} \cdots, t_{ij})$; where t_{ij} denotes a value or cardinal number [196] achieved by the team for the jth subcriterion of the ith criterion.

6. Finally, the **sixth column** (Table 6.16) denotes the team's overall score (O) for the jth subcriterion of the ith criterion. This is computed as $O = w_{ij} \times t_{ij}$.

An analyst's overall performance score (X) is computed using Equation 6.5 below:

$$X = \sum_{i=1}^{6} \sum_{j=1}^{N_i} S \tag{6.5}$$

The team's overall performance score (O) is computed using Equation 6.6:

$$Y = \sum_{i=1}^{6} \sum_{j=1}^{N_i} O \tag{6.6}$$

An analyst's percentage contribution (Z) to the team is computed using Equation 6.7:

$$Z = 100 \times \frac{X}{Y} \tag{6.7}$$

The SOC-AAM contains two qualitative subcriteria (the quality of analysis and the quality of incident report) that must be scored by a SOC manager or the technical lead. As a part of the evaluation process, a SOC manager needs to review a randomly selected report written by an analyst during an assessment period and assign a score value between 1 to 7 (where 1 is the lowest and 7 is the highest), depending on how many of the seven quality indicators the analyst has addressed in the report (see Figure 6.13). Prior work [55] found that the quality of incident analysis is often reflected in the report written by an analyst [55]. Therefore, the manager could assign the same score to both the quality of incident analysis and the quality of incident report. Alternatively, she or he could choose to assign a different score for the quality of analysis up to a maximum of 7. However, this does not suggest that the quality of analysis is the same as the quality of the report because the research participants assigned different weights for the quality of analysis and the quality of the report.

The steps for evaluating analysts' performance are outlined below and reported in [69]:

- Step 1: The evaluator enters the total number of analysts in the team into the SOC-AAM tool. This will calculate the maximum team score for the quality of analysis and the quality of their report (Note: Each analyst can achieve only a maximum score of 7 for the quality of their analysis and a maximum score of 7 for the quality of their report, based on the seven indicators as stated earlier; the overall team score is, therefore, 7, multiplied by the number of analysts for each of the two functions);

- Step 2: If an analyst produces a report during the evaluation period, the SOC manager or technical lead must analyse it and provide a quality score based on a value between 1 to 7 for the report.

- Step 3: The evaluator must enter the scores (based on a cardinal number) for the remaining functions. Once the evaluator has entered all the scores, the SOC-AAM tool will automatically compute an analyst's overall performance score as shown

in Equation 6.5. Where there are no scores for a particular subcriteria, that should be left blank. For example, in a SOC where analysts do not create use cases, the KPI score value for use cases is simply left blank.

- Step 4: In order to compare an analyst's performance against their peers, the team's total scores for each function must be entered for the evaluation period. The team's performance is computed automatically using Equation 6.6. Once completed, the score for individual analysts would be displayed as a percentage (see Equation 6.7) to reflect their individual contribution to the overall team's effort for a reporting period.

Chapter 7 presents the evaluation of all the artefacts designed in this research.

6.7 Chapter Summary - Conclusion

This chapter presented the functions of analysts as well as metrics for measuring their performance. The chapter also presented the following artefacts: constructs, frameworks, a method and an instantiation of the method. Whereas constructs describe the functions of a SOC and metrics/KPIs for capturing their performance, the SOC conceptual framework presented the functions of a SOC as identified in the existing SOC frameworks validated by the participants as well as functions suggested by the participants. The SOC-AAF presents the functions of an analyst from the list of SOC functions and the metrics for measuring an analyst's performance. The SOC-AAM presents a systematic approach for measuring the performance of an analyst.

The next chapter presents the empirical evaluation of the proposed artefacts and instantiation of the SOC-AAM.

Chapter 7

Evaluation of the Designed Artefacts

7.1 Introduction

Evaluation is an important step in a DSR process as it provides essential feedback on the utility of the design [138]. This chapter presents the evaluation of the artefacts created in Chapter 6 of this thesis. There were three iterations of the design process, as illustrated in Figure 7.1 with each iteration producing an artefact. This approach is consistent with a typical DSR process, which requires a researcher to create a viable artefact through an iterative process to solve the identified problem until the proposed solution and its results are deemed satisfactory by users of the artefact or experts in the domain [132, 227].

The first iteration resulted in the development of constructs and the creation of a SOC conceptual framework for understanding the functions of a SOC and the metrics for capturing an analyst's performance. The constructs and the SOC conceptual framework were used as an input for the second iteration.

The SOC-AAF was created during iteration 2. The SOC-AAF focuses on only the functions of an analyst and maps the analyst's functions to various metrics.

The third iteration was the creation of a systematic method for measuring an analyst's performance that incorporates the proposed guidelines for assessing the quality of an incident analysis and incident report developed in iteration 2.

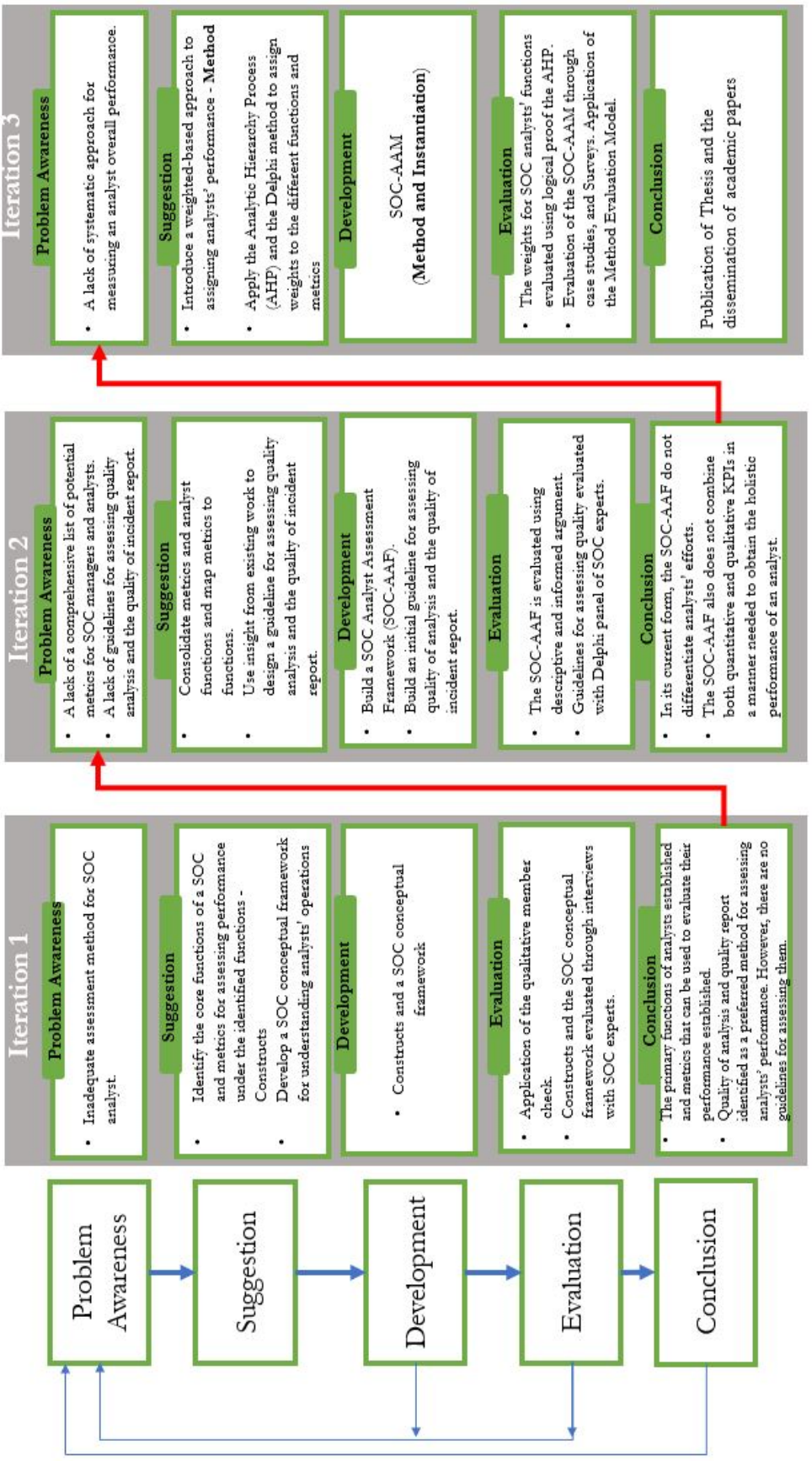

Figure 7.1: DSR Process and Resultant Artefacts

7.2 Reflection on the guidelines for conducting a DSR

This study found it necessary to ensure that the entire research process adhered to the widely applicable guidelines for conducting a DSR [144]. A discussion of how this study adheres to the DSR guidelines is provided below. According to Hevner et al. [144], a DSR must comply with the following seven guidelines:

Guideline 1: Design as an Artefact - Hevner et al. [144] state that the first goal of a DSR is to produce an artefact. An artefact, as mentioned in chapter 3, is a human-made object designed to solve a practical problem [132]. There are numerous artefacts in the literature. These include constructs, models, methods, instantiations, frameworks, architecture, design principles, mathematical formulae, and design theories [132, 144, 228]. The artefacts created in this study are constructs, a framework, a method, and an instantiation.

Guideline 2: Problem Relevance - According to Hevner et al. [144], the second objective of a DSR is to develop a solution to a problem that is meaningful and relevant to a business. There are several justifications in the literature for devising a systematic method for measuring the performance of an analyst [49, 54]. For example, existing literature reports how a lack of a systematic approach to measuring analysts' performance frustrates both SOC managers and analysts working in a SOC [25]. This study, therefore, proposes a method for systematically evaluating the performance of an analyst, based on multiple functions. In addition, there is evidence in the literature suggesting that both novice and experienced analysts suffer from the complexity of security incident analysis tasks [2]. To the best of the researchers' knowledge, there is no formal guideline for supporting analysts conducting their analysis function. This study proposes a guideline that can be used by an analyst during analysis and also to assess the quality of an incident analysis and the presentation of their report.

Guideline 3: Design Evaluation - Once an artefact has been built/designed, the next objective is to evaluate it [229]. Hevner et al. [144] posit that designed artefacts must

be evaluated to demonstrate their efficacy. The purpose of evaluation, as explained by Johannesson and Perjons [138] is to determine how well a designed artefact solves the issue at hand. Various techniques exist for evaluating artefacts in DSR. The evaluation techniques applied in this study are (1) respondent validation (qualitative member checks) through interviews, (2) logical proof of the AHP decisions to determine the consistency of the judgement, (3) informed argument, and (4) the application of the Method Adoption Model (MAM) through a case study.

Guideline 4: Research Contributions - The fourth goal of a DSR is to produce a verifiable contribution [144]. This study contributes both academically and practically to the body of knowledge. The study proposes a formal framework that can be used as an educational tool to understand the functions of a SOC and the role of analysts. This framework can also be leveraged by other security researchers interested in learning more about a SOC.

Another contribution is the proposed systematic approach for measuring an analyst's performance. The proposed method represents a shift from the traditional method of evaluating analysts' performance, which does not take into account multiple aspects of their work. This research also provides a novel guideline for assessing the quality of an incident analysis and report by analysts, which is incorporated into the measurement method.

Guideline 5: Research Rigour - The fifth guideline is the application of a rigorous research process based on existing theories, constructs and experiences to design an artefact [144]. Johannesson and Perjons [138] assert that the DSR must utilise rigorous research methods. This study uses the existing SOC frameworks and models to build a systematic approach for measuring an analyst's performance. Additionally, the research draws on well-established research methods (interviews, participant observation, document reviews, the Delphi method and the AHP).

Guideline 6: Design as a Search Process - The sixth objective of the DSR is to search for and investigate potential solutions that can be used to solve the practical

problem identified [144]. This research explored various literature on SOCs to identify any framework or model that can be used to design an approach for measuring an analyst's performance. Having established the functions of analysts and the metrics for measuring an analyst's performance, a thorough search of existing theories was conducted to identify a systematic way of integrating the different metrics. The AHP was identified as a useful framework that can be used to synthesise subjective and objective metrics to measure the overall performance of an analyst. To the best of the researcher's ability, this study is the first of its kind to re-contextualise the AHP into a SOC setting and specifically to measure an analyst's performance.

Guideline 7: Communication of Research - The final objective of a DSR, according to Hevner et al.[144], is to communicate the output via scholarly publication to researchers and practitioners in the field [138]. Johannesson and Perjons [138] state that disseminating the results allows other researchers to evaluate the artefact and build on it. They say that a researcher needs to communicate the output of DSR to both technology-oriented and management-oriented audiences. The output of this research was shared with academics and practitioners in the field of SOC during cyber security conferences, workshops and poster day events. Additionally, a number of research articles were published as part of this research [24, 49, 55, 69].

7.3 Evaluating Proposed Artefacts

Peffers et al. [230] reviewed 148 DSR papers and identified eight common evaluation methods for designed artefacts. Amongst them are case studies, field studies, experiments, simulations, informed arguments, focus groups, interviews, and logical proof [138, 230]. Table 7.1 shows the evaluation approaches used in this study.

Table 7.1: Adopted Evaluation Technique

Artefacts	Adopted Evaluation Technique
Constructs	Interviews and the application of the qualitative member check
The SOC Conceptual Framework and the SOC-AAF	Interviews and informed argument
The SOC-AAM	Logical proof using the AHP consistency index and the application of the Delphi method
An instantiation of the SOC-AAM	A case study and the application of the Method Adoption Model (MAM)

7.3.1 Iteration 1: Evaluation of the Constructs and the SOC Conceptual Framework

The constructs from Chapter 6 were evaluated using the member check technique during the interviews. The member check technique (also known as respondent validation) involved showing the study participants the output from the interview data or sections of the recorded data to check for accuracy and resonance with their experiences [183]. The responses from the participants are then recorded to validate the information captured by the researcher as part of the interview.

The interview results were used to create constructs, consisting of the functions of a SOC and the responsibilities of an analyst. The SOC experts participating in the interviews were requested to comment on the constructs in terms of their coverage of the functions of a SOC, the functions of an analyst, and the main metrics for measuring an analyst's performance. Presenting the constructs to participants offered them the opportunity to confirm or reject certain parts of the framework. As stated in Chapter 6

Section 6.2.5, the constructs were organised into a SOC conceptual framework shown in Figure 6.1 and was presented to the interview participants. The participants were asked to comment on the constructs and the proposed SOC conceptual framework using the following question:

Question: The template/framework is intended to represent the functions of a SOC, identify the functions of an analyst and performance metrics for analysts. In your opinion, is there anything that you would like to add in terms of the functions or areas of measure?

As reported in Chapter 6 under Section 6.2.1, the thematic analysis is used to analyse the interview data. Under thematic analysis direct quotes and paraphrasing from interview data are used to report and support the findings from a study [231]. Aronson [231] states that using direct quotes and paraphrasing also increases the credibility of the study's findings. Table 7.2 presents the feedback received from the participants on the constructs.

Table 7.2: Perceived Completeness of the Constructs and Conceptual Framework

Participant	**Response**
Participant 1	*I can't think of anything else in terms of the SOC functions. Maybe a containment function? But I suppose that will come under incident management. I don't think there is anything else you can add to your framework.*
Participant 2	*Unless it is part of the intelligence function or part of the response, interaction with other organisations like the 5 Eye community, which is one of our functions...But generally, your framework is good.*

Table 7.2 – continued from previous page

Participant	Response
Participant 3	*If you are looking at the activities of a SOC, I think you've covered everything that our SOC carries out. I don't think there is anything out there that we could do. It does look complete and mirrors the separate departments in our SOC.*
Participant 4	*Most SOC functions fall under one of those categories anyway. I think your framework covers all the areas that can be measured.*
Participant 5	*Your framework covers all SOC functions. Obviously, the monitoring and detection function and the analysis function are the two major ones. The framework is pretty good and covers all the functions of a SOC.*
Participant 6	*You have covered a lot of the basics. Nothing that shouts out. I don't think there is anything that we do in our SOC that is not in this framework. I think it's all covered.*
Participant 7	*It is very foundational. I don't think there is anything out there that jumps out that is not covered. Yeah, I think the framework covers it very well.*
Participant 8	*I don't think there is anything else. For a SOC itself, it covers it.*
Participant 9	*I can't see anything from the top of my head, depending on what you are offering to the customer, but to be honest, I think you've got it covered, what should be offered as a service and the functional areas that should be covered.*
Participant 10	*I think these are the main functions of a SOC.*
Participant 11	*To be honest with you, you do have the full spectrum there.*

Table 7.2 – continued from previous page

Participant	Response
Participant 12	*On the functions, I believe your framework covers almost everything.*

The above feedback from the SOC experts who took part in this study shows that participants believe the constructs cover the functions of a SOC and the work of an analyst. The responses from P4, P5, P6, P8, P9, P10, and P11, in particular, indicate that an organisation providing a SOC service will provide one of the functions outlined in Figure 6.1.

7.3.2 Iteration 2: Evaluation of the SOC-AAF

In collaboration with the interview participants, the constructs were used to create the SOC-AAF as discussed in Section 6.3. The SOC-AAF consolidates analysts' functions and maps each function to a range of metrics reported in the literature and those suggested by the participants. The criteria used for designing the SOC-AAF is presented in Section 6.3.1

The SOC-AAF was evaluated using informed argument [230, 232]. The adopted evaluation process in this iteration is similar to the strategy reported in [233, 234] which relies on informed argument. An informed argument is the process of using existing relevant research and literature to build a convincing argument for the artefact's utility [232]. Hevner et al. [144] posit that the existing knowledge base can be used to build an informed argument regarding the usefulness of an artefact.

However, relying on an existing knowledge base or utilising the existing literature to build an argument on the utility of an artefact is akin to using secondary data sources and

thus has some disadvantages. For example, Rose et al. [155] opine that because existing works were designed and intended to find answers to a different problem, they may not answer the researcher's specific research questions or contain specific information that the researcher desires. Nonetheless, as reported in [64] existing works can still be useful in helping researchers answer certain research questions and test some hypotheses. In addition, secondary data sources provide a time-efficient and easily accessible source of information for research [64, 235].

The SOC-AAF was evaluated using the criteria used by Albluwi [234] to evaluate his framework for performance evaluation of Computer Security Incident Response (CSIR) capabilities. Albluwi's [234] work is relevant because of its similarities to the activities of a SOC. Albluwi's [234] evaluated his CSIR framework against three attributes: comprehensiveness, flexibility, and compatibility. In this study, these three items were complemented with additional attributes suggested in [236] as the criteria for a good enterprise framework. Since a SOC and the role of analysts fall within an enterprise activity [28], this study opines that a framework built for a SOC, or for that matter analysts, can be evaluated against enterprise framework attributes. The additional attributes complementing the attributes proposed by Albluwi are assessing the simplicity of the framework and its practicality [237].

The SOC-AAF was therefore evaluated against the following attributes: (1) Simplicity, (2) Comprehensiveness, (3) Flexibility, (4) Compatibility, and (5) Practicality:

- Simplicity - This attribute indicates that the framework is simple to understand and easy to use [238]. Indeed, according to the DSR process, artefacts need to be evaluated for their simplicity, understandability and ease of use [229, 238]. The SOC-AAF is simple and easy to understand. This is because the constructs used within the framework resonates with SOC practitioners and SOC researchers. It is also simple because it is based on the functions of a SOC and the functions that an analyst is expected to perform as reported by the participants and as such practitioners can easily understand it and relate to it. Many of these functions can

also be found in the existing SOC frameworks [21, 52].

- Comprehensiveness - While there is no clear definition or outline of what constitutes comprehensiveness of a framework [234], some scholars argue that a comprehensive framework must be detailed and must include pertinent constructs congruent with the domain [237, 239]. In this study, the SOC-AAF was developed following a thorough analysis of the literature and through engagement with SOC experts. Engaging with the literature and practitioners was to ensure that the relevant constructs required to capture the performance of an analyst were documented. The SOC-AAF covers the most common functions expected of an analyst according to the study participants [55] and as reported during the evaluation of the Iteration 1. The comprehensiveness and completeness of the overall method was also evaluated by the SOC experts. The existing SOC frameworks also contain the functions in the SOC-AAF [21, 52].

- Flexibility - Flexibility denotes the framework's applicability and adaptability to the operations of different SOC settings [240]. The flexibility argument is based on participants' suggestion that the framework contains all the major SOC functions, thus it offers a flexible means of representing the range of analysts functions in different SOCs. SOC system designers can also use aspects of the framework in their research where analysts are not accessible to them.

- Compatibility - This means the framework can coexist with other SOC frameworks [241]. The SOC-AAF is grounded in existing works and more specifically the existing SOC frameworks. To that end, it is compatible with existing SOC frameworks when trying to understand the functions of a SOC. As with the existing frameworks the SOC-AAF can also be used to explain the functions of a SOC albeit it focuses is on the functions performed by analysts. The SOC-AAF also presents a range of metrics for measuring the performance of an analyst.

- Practicality - This implies that the framework can be put into practice successfully [237]. The SOC-AAF is a practical framework that supported the researcher's

efforts to design a method for measuring the performance of an analyst. The SOC-AAF aids in identifying the key areas of measurement for analysts to achieve the overall aim of this project.

7.3.3 Iteration 3: Evaluation of the SOC-AAM

The SOC-AAM was presented to SOC practitioners for an empirical evaluation. It is important to note that the guidelines for assessing the quality of incident analysis and the quality of an incident report that comes with the SOC-AAM were evaluated as part of the Delphi study by the experts. Peffers et al. [230] assert that the Delphi method is an effective evaluation method because it allows experts to provide their individual opinions on a topic.

The evaluation of the SOC-AAM was in two parts: **a preliminary evaluation** and **an extensive evaluation**. The preliminary evaluation was a rapid test to determine the feasibility of using the SOC-AAM as an evaluation tool in a SOC; it was also an opportunity to determine the feasibility and suitability of using a weighted approach to evaluate an analyst's performance. Furthermore, the preliminary evaluation provided preliminary feedback for improvement. A questionnaire based on the MAM was used in an extensive evaluation involving more participants and different SOCs to assess the efficacy of the SOC-AAM in four dimensions (perceived usefulness, ease of use, intention to use, and completeness).

7.3.3.1 Preliminary Evaluation of the SOC-AAM: Experts' Feedback

During the preliminary evaluation, the SOC-AAM template (Table 6.15) was presented to the SOC supporting this study for an initial assessment. To protect the identity of the organisation and analysts that took part in the preliminary evaluation, the participating organisation SOC is referred to as 'Corp1-SOC'. Corp 1-SOC provides security monitoring and response services to a multinational aerospace organisation that designs,

manufactures and sells commercial and military aircraft. They also offer SOC services to other organisations in the form of an MSSP.

Following a meeting with the Corp1-SOC management team, two senior analysts and the SOC manager agreed to evaluate the usability of the SOC-AAM and provide feedback. The participants were given a participant information sheet that explained the objective of the study, their rights; and the option to participate in the study or not. The analysts and their managers were given a demonstration of the SOC-AAM, using hypothetical values or metrics scores as per the SOC-AAM design. As an example, where an analyst has closed two high priority incidents and opened three medium priority incidents, scores of 2 and 3 will be allocated respectively in the SOC-AAM under the appropriate fields in the SOC-AAM. Following the demonstration, the analysts were free to either enter their achieved metrics as they accomplished them or collect that information from their ticketing systems at the end of their shift cycle to complete the SOC-AAM. The two analysts decided to enter their metrics as they achieved them. The testing lasted for approximately 5 hours; and at the end of the exercise, the participants were requested to submit their Excel spreadsheets to their manager and the researcher. The manager also used the information from the team's ticketing system to populate the SOC-AAM in order to evaluate the performance of the team members.

At the end of the testing, the participants were given a short open-ended questionnaire in which they were requested to provide feedback on the general usability and usefulness of the weighted approach [229]. The participants were also requested to share their thoughts on using the SOC-AAM tool. There were two questions capturing the opinion of the participants:

Question 1 (Q1): Can you please comment on the general usability and usefulness of the attached assessment method?

Question 2 (Q2): Can you please summarise your experience and overall thoughts on the assessment framework?

The overall preliminary feedback obtained from the SOC manager and analysts who tested the SOC-AAM tool suggests that the SOC-AAM is useful and easy to use. The feedback received are as follows:

Analyst 1:

Q1: This is a very helpful tool, and I had no trouble using it. Once you get used to the layout, it is actually pretty easy to use. Worked well.

Q2: From a senior analyst perspective, the spreadsheet is easy to understand, and the data required from analysts, or a manager also looks straightforward to me. This framework can easily be used to compare the performance of two people.

Analyst 2:

Q1: I found this tool fairly useful, thanks to the inclusion of the readme.

Q2: I found it to be very user-friendly, and the quality of analysis guideline contains a wealth of information. I am satisfied with it as a tool for assessing performance because it allows you to compare the performance of team members.

The SOC manager:

Q1: In my position as the SOC Service Delivery Manager, I often collate statistics on a regular basis. I have reviewed the reporting tool created by Enoch, which demonstrates individual analysts and combined Team performance totals. I believe that this will be useful as not only a time saving exercise for Managers to report on the performance statistics, but will also be able to identify strengths and weaknesses for individuals or the team as a whole, which in turn will help to identify areas where training will be beneficial.

I found this tool easy to use and to work with, once verbally explained. I would suggest that an extra tab should be added with a set of instructions, to cover the 'Single Point Of Failure' aspect, as in if the monitoring or reporting has to be taken over by someone who is unfamiliar with using the spreadsheet.

The 'Criteria For Quality Analysis' would also be handy to give to the Team members. The individuals would be aware of exactly what they are being assessed on and also the areas they need to keep in mind when working on tasks.

Q2: My overall thoughts are that this would prove to be a useful tool for reporting, identifying areas of training and focus on performances of the team.

I can see that a lot of hard work and thought has gone into the spreadsheet which has taken in all aspects of the SOC environment which a Manager would find extremely useful.

However, due to the small sample size, more detailed testing was conducted using the MAM [242, 243]. As a result, additional testing (extensive testing) was carried out. The testing took place at two different organisations over a four-month period. One of the organisations was Corp1-SOC (used for the preliminary testing), and the other is referred to as Corp2-SOC to anonymise the organisation. Corp1-SOC provides a 24x7 security monitoring and response service for its own organisation and also offers a Managed Service Security Provider (MSSP) to a number of other organisations in the United Kingdom and across Europe. Twelve analysts from Corp1-SOC, the team manager, and the technical lead (who is also a deputy manager) took part in the study without any reward for participation.

Corp2-SOC is responsible for providing internal SOC service at a large telecommunication firm in Norway. The manager at Corp2-SOC, along with two analysts, participated in the testing and evaluation of the SOC-AAM.

Full details for the performance assessment scores from the testing can be found by following the link below:

https://git.cardiff.ac.uk/c1854157/analysts-performance-scores.git

The SOC managers and analysts were requested to evaluate the SOC-AAM and its overall utility based on their professional judgement using the MAM. The MAM is a

theoretical model for evaluating a designed method. The section below presents the findings from the extended testing.

7.3.3.2 Extensive Evaluation via the Application of the Method Adoption Model

The extended evaluation was guided by the MAM, which is derived from the Method Evaluation Model (MEM). The MEM is a theoretical model for validating IS design methods [152]. However, as explained by Paz et al. [242], the MEM has general aspects of evaluation that can be applied to any design method. The MEM consists of six constructs whose relationships are shown in Figure 7.2.

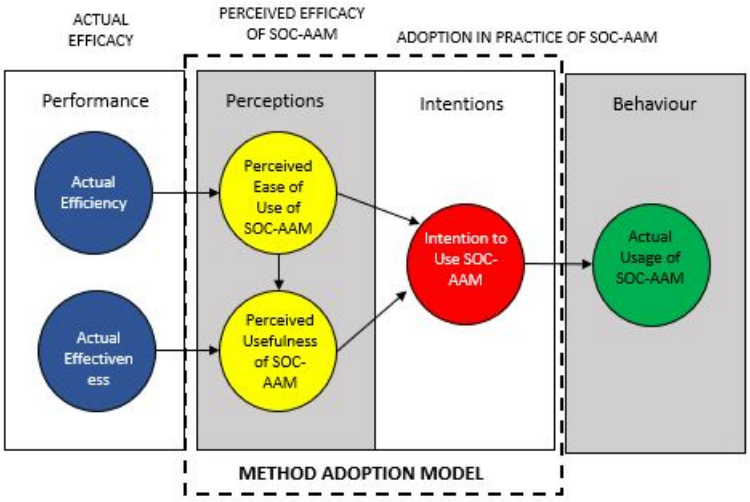

Figure 7.2: The Method Evaluation Model [152]

The definitions for the MEM constructs which we adopted [152, 239, 242] are as follows:

- Actual Efficiency: refers to the effort required to apply a method;
- Actual Effectiveness: denotes the degree to which a method achieves its objective;
- Perceived Ease of Use (PEOU): refers to the degree to which a person believes that using a method would be free of effort;

- Perceived Usefulness (PU): denotes the degree to which a person believes that a particular method will be effective in achieving its intended objective;
- Intention to Use (ItU): denotes the extent to which a person intends to use a particular method; and
- Actual Usage: represents the extent to which a method is used in practice.

While the MEM has six constructs, the evidence from the literature indicates that one does not have to use all of them when evaluating a design method, as some of the elements may not be appropriate in certain situations [69, 152, 244]. This research focused on the perception/intention-based constructs of the MEM known as the MAM [242, 244, 245, 246, 247]. According to Abrahào et al. [248], one of the major advantages of using the MAM and the associated measurement scales is that they are based on previous studies in which similar surveys were used and validated in the context of method adoption.

The strategy used in this study is similar to the work of Paz et al. [242, 249], Recker et al. [244], Pow-Sang et al. [246], Díaz et al. [250, 251], Abrahào et al. [252] and Condori-Fernandez and Pastor [245] in that only sections of the MEM are used. The reasons for this are as follows. Firstly, Moody [152] states that it is not possible to evaluate 'Actual Usage' under experimental conditions. Given that the evaluation was conducted as part of an experiment, it is not feasible to test actual usage [152]. However, scholars argue that an intention to use a particular method can be a predictor of 'Actual Usage' of the method [242, 244]. So, although the 'Actual Usage' construct is not used as part of the experiment, this study argues that an expression of intent by SOC practitioners to use the SOC-AAM in the future demonstrates the likelihood of the SOC-AAM being adopted and used in practice.

Secondly, Moody asserts that using the 'Actual Efficacy' constructs only makes sense when comparing methods [152]. Given that the SOC-AAM is new and, to the author's knowledge, the only existing systematic method for measuring an analyst's performance

- it cannot be compared to any other systematic method. The SOC-AAM is unique in that it incorporates various functions and well-defined guidelines for assessing the quality of an incident analysis and the quality of incident report that do not currently exist. This study, therefore, does not use the 'Actual Efficacy' constructs.

In addition to the MAM constructs, this study also solicited the opinions of the SOC experts on their 'Perceived Completeness' (PCO) of the SOC-AAM [242, 243]. 'PCO' is defined as the extent to which a SOC expert believes that the SOC-AAM covers all aspects of an analyst's functions [242]. Also, SOC managers' and analysts' opinions were solicited to ascertain whether the SOC-AAM resulted in any observed improvement in an analyst's performance. Lastly, SOC managers were also asked to confirm whether their analysts' scores reflected their true performance from the manager's perspective during the experiment.

The extended evaluation was guided by the research questions (RQ-A1 to RQ-A5) listed below. RQ-A1, RQ-A2 and RQ-A3 were adopted from previous studies [242] and adjusted to the context of this study. RQ-A4 and RQ-A5 were specifically designed to ascertain whether the introduction of the SOC-AAM leads to an improvement in an analyst's performance and whether the scores achieved by each analyst measured using the SOC-AAM reflect their manager's perception about their performance in the team.

- (RQ-A1) Do SOC managers and analysts consider the SOC-AAM easy-to-use and useful?
- (RQ-A2) Would SOC managers and analysts use the SOC-AAM in practice in the future?
- (RQ-A3) According to the SOC managers and analysts, to what extent does the SOC-AAM cover all the main functions of an analyst?
- (RQ-A4) According to the SOC managers and analysts, did the introduction of the SOC-AAM lead to an improvement in an analyst's performance?

- (RQ-A5) According to SOC managers, did the final performance score(s) of analysts in their team reflect the manager's perceived performance of each analyst?

The MAM constructs were operationalised, using multiple indicators to devise a questionnaire. The questionnaire was used to collect empirical data from the SOC experts who participated in the testing of the SOC-AAM. The items of the questionnaire instrument were formulated using a 5-point Likert scale. The items on the survey were constructed by synthesising previous measurement items from the literature [152, 242, 253, 254]. For each item on the survey, the participants were asked to rate their responses on a five-point scale, ranging from 1 to 5, where 1 denotes an extremely negative perception of the construct and 5 represents an excellent positive rating. The outcome of the questionnaire was also used to test the hypothesis defined in Chapter 1 under Section 1.2.2.

The constructs and original scales adopted for the study are shown in Table 7.3.

Table 7.3: Constructs and original scales adopted for the study

Construct	**Adopted construct definition**	**No**	**Item**	**References**
Perceived Usefulness (PU)	The extent to which a person believes that the SOC-AAM will be effective for evaluating the performance of an analyst.	PU1	Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	Adopted from: [152](PU4, Q7) [239] (PU1, Q1) [253] (PU14)

Table 7.3 – continued from previous page

Construct	Adopted construct definition	No	Item	References
		PU2	I find the SOC-AAM useful for achieving the purpose of measuring an analyst's performance.	Adopted from: [239] (PU1, Q2)
		PU3	The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	Adopted from: [152](PU6, Q12)
Perceived Ease of Use (PEOU)	The extent to which a person believes that using the SOC-AAM would be free of effort.	PEOU1	I found the procedure for applying the SOC-AAM easy to follow.	Adopted from: [152](PEOU1, Q1) [253] (PEOU14)

Table 7.3 – continued from previous page

Construct	Adopted construct definition	No	Item	References
		PEOU2	Overall, I found the SOC-AAM easy to use.	Adopted from: [152](PEOU1, Q4) [239](PEOU1, Q1) [253] (PEOU8)
		PEOU3	I found the SOC-AAM easy to learn.	Adopted from: [152](PEOU3, Q6) [239](PEOU3, Q1) [255] (PEOU1, Q26)
		PEOU4	The SOC-AAM is clear and easy to grasp.	Adopted from: [152](PEOU5, Q11) [255] (PEOU2, Q33)
Intention to Use (ItU)	The extent to which a person intends to continue to use the SOC-AAM for the evaluation of an analyst performance.	ItU1	If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	Adopted from: [239] (ItU1, Q1)

Table 7.3 – continued from previous page

Construct	Adopted construct definition	No	Item	References
		ItU2	In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	Adopted from: [239] (ItU2)
		ItU3	I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	Adopted from: [239] (ItU3) [152] (ItU2, Q16)

Table 7.3 – continued from previous page

Construct	Adopted construct definition	No	Item	References
Perceived Completeness (PCO)	The extent to which a person believes that the SOC-AAM covers all core areas in evaluating the performance of an analyst.	PCO1	I found the SOC-AAM to be a complete method for measuring the performance of an analyst based on their task performance.	Adopted from: [242]
		PCO2	I found the SOC-AAM to be a complete method for measuring an analyst's performance in comparison to existing approach.	Adopted from: [69]

Prior to the testing, the managers were each given a practical demonstration on using the SOC-AAM tool via Zoom. During the demonstration, hypothetical metric values

were used to illustrate how to use the tool for an evaluation. Although a demonstration was provided, the SOC-AAM tool was accompanied by "Read Me" notes detailing a step-by-step process regarding its use.

7.3.4 Results of Post-Testing Feedback

After four months of testing, the participants were invited by email to participate in a post-testing survey (see Appendix K). A link to the online survey questionnaire was included in the email. All the participants (17 in total) completed and returned the questionnaire. The feedback received from the participants was used to answer the research questions defined under section 7.3.3.2. The results from the testing are presented below.

7.3.4.1 Reliability Analysis of the Questionnaire Items

The Cronbach's alpha was used to analyse the reliability and internal consistency of the set of scale items used in the survey. The measurement of Cronbach's alpha is usually reported as a value between 0 and 1 [208]. Although there is no agreed-upon standard for reliability, in the literature, $\alpha \geq 0.7$ is typically considered to be acceptable [152]. Majid et al. [208] also point out that a value closer to 1 indicates a high level of reliability and internal consistency of the items.

The results show that all areas have an alpha value greater than 0.7 (see Table 7.4). This implies that the items in the questionnaire are highly correlated.

Table 7.4: Reliability of the Scale Items

CONSTRUCT	CRONBACH'S α
Perceived Ease of Use	.886
Perceived Usefulness	.894
Intention to Use	.899
Perceived Completeness	.761

7.3.4.2 (RQ-A1): Perceived Ease of Use and Perceived Usefulness

This section addresses research question (RQ-A1), which is defined in section 7.3.3.2. It also investigates **Hypothesis 1**, defined in Chapter 1 under Section 1.2.2 which postulates that:

The SOC-AAM is an easy to use and a useful method for measuring the performance of an analyst $(H.a_1)$.

Under the MAM/MEM, a score greater than 3 (the neutral point in a 5-point Likert scale) indicates a positive perception [242, 244, 256]. A Likert scale is a rating scale used to measure opinions, perceptions, attitudes and/or behaviours of research participants [257, 258]. The aim was to analyse the survey data to determine whether the overall perception rating from the participants was greater or less than 3 for the various constructs.

A Shapiro-Wilk normality test [259] using SPSS revealed that the data from the participants was not normally distributed as the $p - value$ was less than 0.05. Appendix M shows the survey responses from the participants. As a result, a non-parametric statistical method was used to test the data.

A non-parametric method also fits the data collected because of the small sample size [256]. The Wilcoxon signed-rank test (a non-parametric test) [260] was used to determine whether the observed median score of the participants was greater than the zero point of the 5-point Likert scale ($\text{median}_0 = 3$) [256]. Table 64 - Appendix M

presents the descriptive statistics of the responses.

The null hypothesis states that observed median scores are less or equal to the zero point (H_0 median$_{variable} \leq$ median$_0$) and the alternative hypothesis states that observed median scores are greater than the zero point (H_A: median$_{variable} >$ median$_0$) [256].

The test result revealed that the median of the scores received from the participants for both PEOU and PU was significantly greater than 3, a $p < 0.05$, indicating that SOC experts had a positive perception of the SOC-AAM. The median scores for the PEOU and PU were 5 and 4, respectively. Tables 59, 60 and 61 (Appendix M) show the overall participants' responses and the mean and median scores for the PU and PEOU respectively.

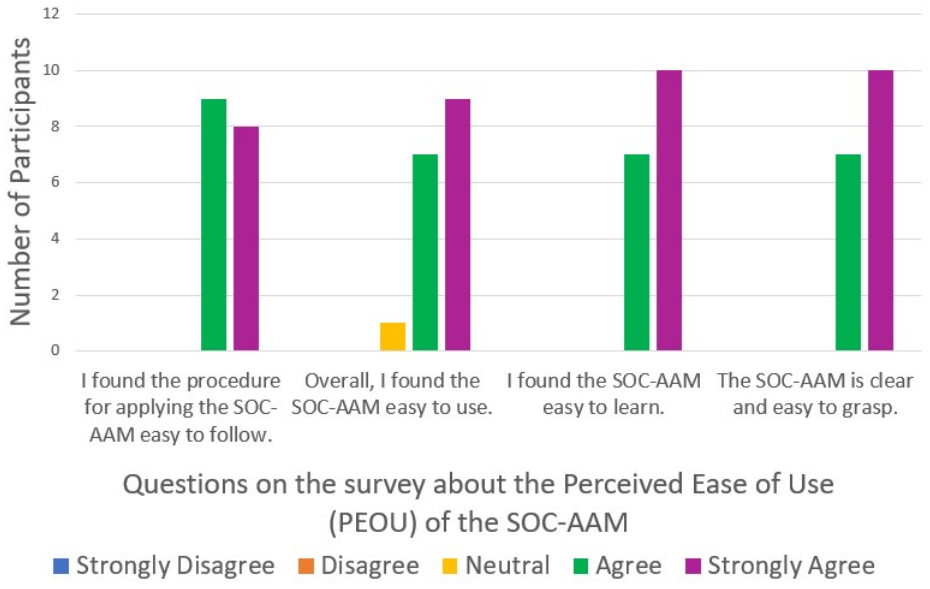

Figure 7.3: Response breakdown regarding the PEOU

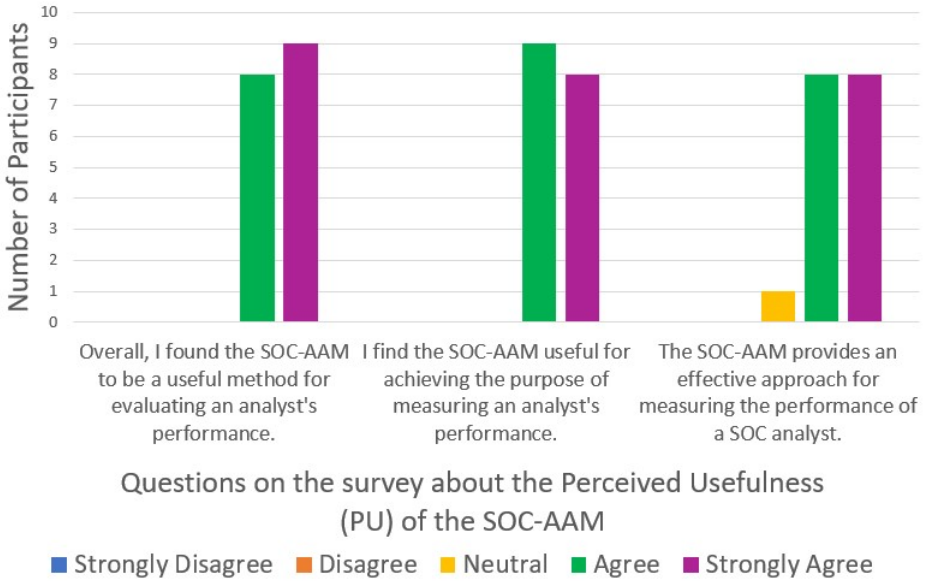

Figure 7.4: Response breakdown regarding the PU

7.3.4.3 (RQ-A2): Intention to Use SOC-AAM in the future

This section addresses research question A2 (RQ-A2), defined under section 7.3.3.2. It also investigates **Hypothesis 2**, defined in Chapter 1 under Section 1.2.2 which postulates that:

SOC managers and analysts will use the SOC-AAM in future $(H.a_2)$.

The intention to use a particular method is considered an important factor when evaluating the pragmatic success of a method. The null hypothesis states that observed median scores concerning practitioners' intention of using the SOC-AAM for future evaluation is less or equal to the zero point (H_0 median$_{variable} \leq$ median$_0$) and the alternative hypothesis states that observed median scores are greater than the zero point (H_A: median$_{variable} >$ median$_0$).

The median score from the participants was 5, which is greater than 3 with a $p < 0.05$. Based on the findings, this research concludes that the participants intend to use the

SOC-AAM in future evaluations. Tables 59 and 62 (Appendix M) show the overall participants responses and the mean and median scores on the ItU.

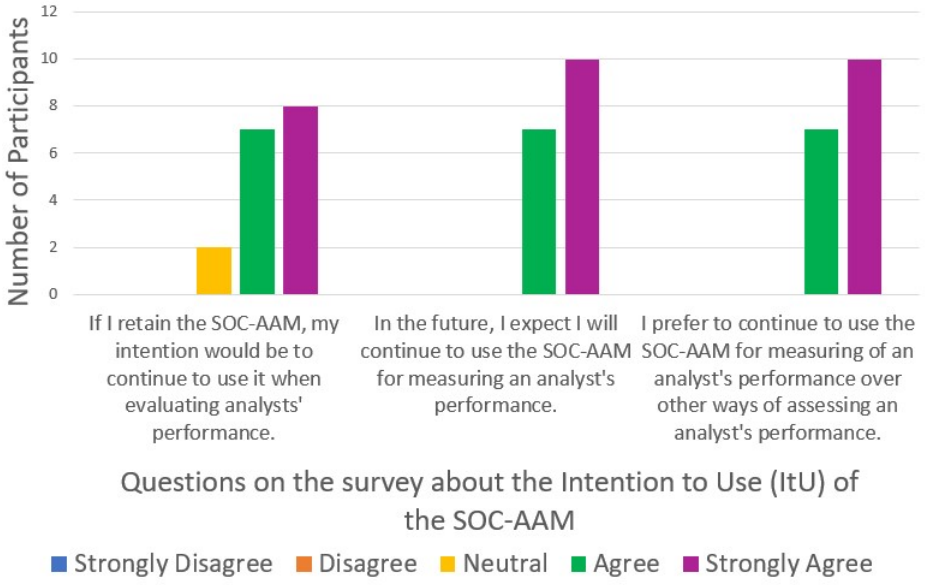

Figure 7.5: Response breakdown regarding the ItU

7.3.4.4 (RQ-A3): The completeness of the SOC-AAM

This section addresses research question A3 (RQ-A3). It also focuses on **Hypothesis 3**, defined in Chapter 1 under Section 1.2.2 which postulates that:

SOC managers and analysts would perceive the SOC-AAM as a complete method for measuring the performance of an analyst $(H.a_3)$.

The participants were asked about how complete they perceived the SOC-AAM as an evaluation tool and their responses showed that they perceived the SOC-AAM as covering the key areas upon which an analyst's performance can be measured. Figure 7.6 shows the results of the PCO.

The null hypothesis states that observed median scores are less or equal to the zero point (H_0 median$_{variable} \leq$ median$_0$) in regard to how the practitioners perceive the

completeness of the SOC-AAM and the alternative hypothesis states that observed median scores are greater than the zero point (H_A: median$_{variable}$ > median$_0$).

The median score for the PCO is 4, which is greater than 3 with a $p < 0.05$. Tables 59 and 63 (Appendix M) show the overall participants' responses and the mean and median scores on the PCO.

While the SOC-AAM was initially conceptualised using existing SOC frameworks [21, 27, 52] and input from SOC experts obtained through interviews, some of the participants reported in their feedback under research question 4 that analysts could be tasked with work that may take time, but that is not accounted for in the SOC-AAM. This may be attributed to the fact that only a small group of people selected the role of an analyst. As a result, some functions might have been overlooked. It is also possible that a different group of experts may have also proposed an additional set of analyst's functions.

Nonetheless, the goal of this study was to propose an approach based on the most common analyst's functions, as reported by a group of SOC experts, and based on the existing framework for understanding the operations of a SOC. Given that all of the functions proposed by the participants in this study also appeared in the SOC framework, this study contends that the analysts' functions used corroborate with the existing understanding of a SOC's role.

It is important to mention that, whereas fourteen people from Corp1-SOC participated in the testing and evaluation of the SOC-AAM, only three people from Corp2-SOC participated in the testing and evaluation. Unfortunately, the sample size from Corp2-SOC was too small for subgroup analyses and as a result, the decision was made to present the results from the two organisations together.

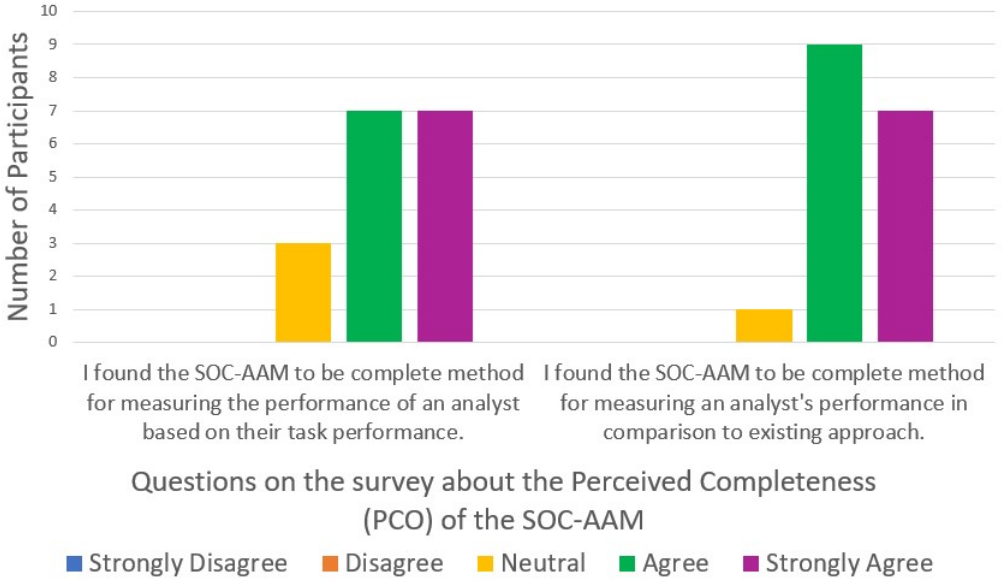

Figure 7.6: Response breakdown regarding the PCO

7.3.4.5 (RQ-A4): Research Question A4

When participants were asked whether the introduction of the SOC-AAM as an evaluation tool resulted in an improvement in an analyst's performance, the proposed guidelines yielded some interesting results.

The SOC manager at Corp1-SOC commented that: *"The guidelines for assessing the quality of analysts' analysis has been useful to the team. I think it encouraged them to expand their thinking and take a step back to think through what they need to do when writing their incident report. I also believe that the tool made it possible for everyone within the team to understand the basis upon which they are being assessed."* The manager at Corp2-SOC was also of a similar opinion but emphasised that producing a good quality report comes with experience. The manager at Corp2-SOC stated that: *"I think the SOC-AAM greatly helped my analysts develop their ability to analyse events. I think the quality of analysis criteria is good, but it comes with experience, knowledge, and the organisation's process."*

The participants said that the guidelines had a positive impact on their analysis and

report writing. Table 7.5 shows the comments from the participating analysts as reported in Appendix L.

Table 7.5: Analysts' statement on whether the SOC-AAM resulted in an improvement in their performance

Participant	Response
Corp2-SOC Analyst 1	*I am very happy using this method because it concentrates on the area of my work that can be measured. I will say it is tangible. I am also happy that the weights for the different tasks are not the same because when I work on high priority incidents, I don't want to have the same score as someone who is only working on low priority incidents. I also think that the how, when, what, who, and recommendation are useful when it comes to incident analysis and helped during my analysis.*
Corp2-SOC Analyst 2	*From what I have done in this assessment, the criteria for quality analysis allowed me to understand a more comprehensive and procedural process of analysing events. It also showed me the area that still needs to improve from the 7 steps of incident analysis processes.*
Corp1-SOC Analyst 1	*I found using the SOC-AAM guidelines useful as it streamlined my work focus, which, in my opinion, made me much more efficient. Overall, I think the tool improved my performance.*
Corp1-SOC Analyst 2	*I think it made it easier to rate my overall performance in terms of the functions listed on the SOC-AAM. I also think that the guidelines provided by the SOC-AAM made it easier when analysing packets. So, I will say that it positively impacted my performance.*

Table 7.5 – continued from previous page

Participant	Response
Corp1-SOC Analyst 3	*Overall, I think the SOC-AAM is a good and a simple tool to use. I like the way it breaks down the different functions, so I can easily see the areas that I did well.*
Corp1-SOC Analyst 4	*Even though log analysis is not something new to me, I found the criteria that you have for assessing the quality of the analysis really useful. In my opinion, those criteria definitely had some impact on my thinking process.*
Corp1-SOC Analyst 5	*The SOC-AAM did not improve my performance in terms of what is expected of me as an analyst.*
Corp1-SOC Analyst 6	*While it felt satisfying to know exactly what I am being assessed on, my concern is that there are still a number of things that take a lot of my time that are not reflected in the SOC-AAM. For example, replying to emails and responding to phone calls.*
Corp1-SOC Analyst 7	*I think the SOC-AAM is useful, especially the who, when, how, what criteria, which I believe helped my thinking process and showed me how to take in a lot of information from an incident and organise them in concise steps when writing my report.*
Corp1-SOC Analyst 8	*In my opinion, although I found the SOC-AAM easy to use, I still think that when I am being asked to work on things that are not in the SOC-AAM, I wouldn't achieve any score, but to be fair, it covers all the major functions we are expected to do and would say it improved my performance in the areas I am being measured on.*

Table 7.5 – continued from previous page

Participant	Response
Corp1-SOC Analyst 9	*In my opinion, the guidelines included in the SOC-AAM helped me to improve on the kind of information that I would have normally included in my report.*
Corp1-SOC Analyst 10	*The SOC-AAM has helped me to improve my performance as I know the tasks I am being assessed on. The criteria for quality analysis bring everything together nicely.*
Corp1-SOC Analyst 11	*I actually think that having this tool is good but it takes a lot of time to fill this form with all these statistics especially when we are busy. Maybe if it can be incorporated into our ticketing system it will be much better. As to whether it improved by performance or not, it is hard to say to be honest.*
Corp1-SOC Analyst 12	*I think my performance remained the same but I found the guidelines interesting and useful.*

This outcome was very encouraging because although the study's objective was to develop a systematic method for evaluating an analyst's performance, the participants' responses indicated that the guidelines for assessing the quality of an analyst's report benefited the analysts that participated in the study as reported in Table 7.5.

7.3.4.6 (RQ-A5): Research Question A5

When the SOC managers were asked whether the scores achieved by their analysts reflected their perceived view of each analyst's contribution to the team, there was some interesting feedback. The manager at Corp1-SOC stated that: *"There are some*

competitive individuals within the team, so I was expecting those individuals to show that competitiveness. However, looking at the monthly scores, it was great to see that all the analysts did pretty well. I am of the opinion that the scores achieved by each individual analyst are reflective of how I perceive their contribution to the team. One area that I saw improvement across the board is report writing."

The manager at Corp2-SOC, on the other hand, stated that the scores obtained by the analysts in their team only reflected about 95% of their performance. However, from the researcher perspective, the 95% was the manager's subjective view based on his team. There were no additional external or academic literature to support the suggested percentage. According to the manager at Corp2-SOC, there were some tasks that the SOC-AAM did not capture. According to Corp2-SOC: *Implementation and architectural activities are not in the SOC-AAM. Therefore, when the results are collected for each period, there will be times when the outcome will not be linear because an analyst was performing other implementation activities. But overall, when compared to the general SOC, I think the SOC-AAM is satisfactory in measuring analyst performance."* While the comments about the other activities not captured by the SOC reflect how Corp2-SOC operates, evidence from the literature shows that the functions mentioned by the Corp2-SOC manager typically fall outside the scope of an analyst's function [17, 38, 55]. Nevertheless, only a small group of experts selected the analyst's functions, and another group of experts may have selected additional or different functions. This is a limitation to this study. Further limitations to this study are detailed in Chapter 8 under Section 8.5.

7.4 Chapter Summary - Conclusion

The evaluation of the artefacts designed in this study was presented in this chapter. Whereas the constructs and conceptual framework were evaluated, using the qualitative member check, the SOC-AAF was evaluated using an informed argument based on the

enterprise framework evaluation criteria and some suggestions from existing work. The MAM, which is based on the MEM, was used as a theoretical framework for assessing the SOC-AAM in four dimensions (perceived usefulness, ease of use, intention to use and completeness). The evidence from the evaluation revealed that the SOC-AAM offered a useful and ease-to-use method. It also revealed that practitioners are likely to use the SOC-AAM in the future and lastly the SOC-AAM offered a complete method for measuring an analyst's performance. The chapter also identified the guidelines for assessing the quality of an incident analysis and incident reports were well received by the participants. The next chapter presents the conclusion of this thesis, recapping the research's key parts, achievements and outcomes, implications for practice, limitations and potential avenues for future work.

Chapter 8

Conclusion

8.1 Introduction

This final chapter presents the conclusion of the thesis. It provides an overview of the research achievements and outcomes. In addition, the chapter highlights the research implications and the limitations of the study, as well as suggestions and avenues for future research.

Even though many studies have mentioned various performance metrics for analysts, there is a concern that current metrics need improvement as they need to take into account the range of functions performed by analysts. None of the existing studies also provide a systematic approach for measuring an analyst's performance. This creates a gap that needs to be filled.

The DSR process [132] was followed to develop artefacts to address the problem identified in the literature and contribute a formal method (the SOC-AAM) towards addressing this gap. The SOC-AAM was tested at two separate SOCs to evaluate its efficacy.

8.2 Key Achievements and Outcomes of the Research

Below presents key achievements and outcomes of the study:

- This research expands on the existing SOC frameworks [21, 52] and models [147] to solve the current gap in the literature concerning the lack of adequate metrics for analysts and the lack of a systematic approach for measuring the performance of an analyst.
- The study consolidates existing metrics for assessing analysts' performance and provides a new formal approach to measuring analyst performance [69].
- Furthermore, this research re-contextualises the existing AHP [68] to measure the performance of a SOC analyst.
- The study also demonstrates the feasibility of capturing the holistic performance of SOC analysts and provides a blueprint for measuring their performance [69].
- The proposed SOC Conceptual Framework can be used as an educational tool as it presents the main functions of a SOC [55].
- Lastly, this research has provided the researcher with an opportunity to publish two peer-reviewed journal papers, a conference paper, a book chapter, and also attend poster day events and conferences.

8.3 Discussion

Despite the importance of performance metrics for assessing the performance of analysts, a literature review in Section 4.4 indicated that the existing assessment methods for analysts require improvement as they fail to consider several aspects of an analyst's functions. Additionally, the literature highlighted the absence of a systematic method for measuring an analyst's performance, causing frustration for both SOC managers

and analysts. Furthermore, there is a lack of guidelines for assessing the quality of an analyst's analysis and the quality of their report.

To address the aforementioned problems, this study developed a systematic approach for evaluating the performance of a SOC analyst referred to as the SOC-AAM, taking into account the level of importance of each function. This study approached the research problem from an empirical point of view by engaging with SOC experts and using a comprehensive and systematic literature search to identify existing scholarly articles [21, 52, 147] to tackle the problem. The existing SOC frameworks, models and metrics were used as the foundation to create new artefacts for evaluating the performance of analysts. The frameworks proposed by Schinagl et al. [21] and Onwubiko [52] were used as the starting point for the development of the SOC-AAM. The SOC-AAM includes a novel guideline for assessing the quality of incident analysis and incident reports produced by analysts.

Twelve SOC experts (four managers and eight analysts) from five industries were invited to participate in a one-to-one interview to get insight into the responsibilities of an analyst within a SOC from the participants' perspective. The interview was also used to identify the main functions of a SOC which was complemented with document reviews and observations during the SOC visits for the face to face interviews.

The participants reported that, among the eleven SOC functions presented in this thesis in Section 6.2.1, the monitoring and detection function, the analysis function, the response and reporting function were the main functions of an analyst. This finding is pertinent because it is consistent with the work of Onwubiko [52] and Lif and Sommestad [147] who identified these three as the primary focus of a SOC. Given that analysts are central to the operations of a SOC, it should come as no surprise that their primary responsibilities are also a SOC's primary functions. In fact, participants advocated that the assessment method for analysts needed to take these three functions into consideration.

The participants indicated that the penetration testing function, forensic and malware

analysis and the log collection functions [21, 52] fell outside the scope of the tasks expected of an analyst. They mentioned that the penetration testing function is the responsibility of a specialised team of penetration testers. Participants also stated that a forensic and a malware specialist is responsible for the forensic and malware functions. The participants also indicated that the engineering and log collection function is the responsibility of a SOC engineer, not an analyst. The participants suggested that the incident management function together with the compliance and risk management function are an integral part of the monitoring, analysis, and reporting processes. As such, these should not be viewed as separate functions per se. The intelligence, policies, and signature management functions, as well as the baseline and vulnerability management functions, were identified as secondary functions of a SOC; and as such, some SOCs may not provide these functions. This finding confirms the work of Jacobs et al. [30].

A number of metrics, both quantitative and qualitative were reported by the participants as useful for measuring an analyst's performance. However, on their own, the suggested metrics did not provide a way of obtaining a comprehensive and holistic view of an analyst's performance. This is because the individual metrics are not linked to provide an overall performance score. A mathematical model was used in this study to synthesise both quantitative and qualitative metrics. The AHP framework was used to consolidate the metrics and analysts' functions identified in this study to provide a formal approach to systematically measure an analyst's performance. The benefit of using the AHP is that it allows for the inclusion of both subjective and objective assessment criteria. The AHP also provides a robust approach for consensus building within a group of experts [68]. Time-based metrics such as MTTR and MTTD were excluded from the AHP because the participants reported them as a poor measure of performance. The participants explained that time-based metrics often have many variables outside an analyst's control, for example, waiting for third parties to provide additional information about an incident [55].

To design and build the SOC-AAM, the Delphi method [169] was integrated into the AHP framework [68] to assign weights to the main functions of an analyst. Eight (8) SOC experts from five different industries participated in the Delphi study. The different functions and associated metrics were assigned different weights. The weighted approach for measuring analysts' performance was introduced into two SOCs for testing and evaluation as part of an experimental case study.

A survey conducted after four months of testing at the two separate SOCs demonstrates that the SOC-AAM method enables a systematic evaluation of a SOC analyst's performance, taking the level of relevance of each function into account. The results also indicated that the SOC-AAM offers a useful, easy-to-use and comprehensive approach to measuring an analyst's performance.

Unlike current performance metrics, which do not differentiate between analysts' performance [25, 52, 54], the weighted approach proposed by this study enables SOC managers to distinguish between efforts based on alert priority, analysis quality, and their overall score is reported out of 100%. Furthermore, the findings from the survey also revealed that given the opportunity, practitioners would prefer to use the SOC-AAM in future evaluations.

Despite the enormous potential of the weighted approach, in practice, the SOC-AAM does not have weights for every task an analyst is expected to perform. The SOC-AAM measures are based on the most common and significant tasks expected of analysts as reported by the study participants [55, 69]. They are also solely based on the task performance of analysts [59].

While this study has demonstrated that it is possible to measure an analyst's performance systematically, the pairwise comparison performed as part of the AHP was a time-consuming activity that may not be feasible for a SOC to repeat for each evaluation. Hence, a contribution of this work is to simplify this process by proposing weights that SOC managers and stakeholders can use to evaluate an analyst's performance without going through another intense AHP process; the proposed weights can be used because

they were developed through consensus among a group of SOC experts.

8.4 Significance of the Study

Whereas previous studies have identified performance metrics for analysts, none of the academic studies provides a systematic approach for measuring the performance of an analyst or provides a guideline for assessing the quality of incident analysis and incident reports.

This study makes a number of contributions as discussed in Section 1.3. The study has both academic and industry significance as it enhances understanding of the role of analysts, the metrics for measuring their performance, and the methods for systematically capturing their performance. The study provides constructs and the SOC-AAF for understanding the functions of analysts and metrics that could be used to capture analyst's performance. The SOC-AAF presents the main functions that must be considered when measuring the performance of an analyst. The constructs and the SOC-AAF are grounded in the existing SOC frameworks.

The study applied the AHP decision-making procedure with the Delphi method to develop the SOC-AAM through the DSR process. The research developed a relationship between practice and theory through the use of the AHP framework allowing practitioners to establish priority weights for the functions of an analyst. Furthermore, the theoretical models (MAM) was applied in the SOC context enabling SOC practitioners to evaluate the proposed artefact.

8.4.1 Implications for Academic Research

The study contributes to the academic community by first presenting a SLR on the challenges facing SOCs. The output of the SLR provides insight and current knowledge on SOCs. It also opens avenues for other research on SOCs as reported in [49]. In addition,

this study presents constructs in a SOC conceptual framework for understanding the functions of a SOC and the role of an analyst [55]. The SOC conceptual framework can be utilised as an educational tool to educate security researchers and students seeking to understand the operations of a SOC. The SOC conceptual framework introduces the concept of "global" SOC functions which represents a comprehensive list of all the major functions typically expected of a SOC. Another significant contribution of this research is that it builds on the existing SOC frameworks to propose the SOC-AAM. The SOC-AAM was empirically tested to assess its usefulness and efficiency. The constructs (SOC functions, analyst functions and metrics for measuring an analyst's performance) could also serve as the basis for future research and practice as it captures the primary operation of a SOC.

8.4.2 Implications for Practice

This research has demonstrated that it is possible to capture the performance of analysts in a systematic manner. The SOC-AAM provides a useful tool for assessing an analyst's performance. However, it is important to point out that the primary functions of analysts used in the SOC-AAM were selected by only a small group of experts, and as such, it is possible that some functions were overlooked which may mean that in practice some SOCs may have some functions for analysts that is not on the SOC-AAM. Nonetheless, the SOC-AAM offers a flexible method for measuring an analyst's performance because it can be tailored to each SOC's specific circumstances based on the functions and services provided. As a result, SOC managers can choose which specific functions to base their analysts' performance on. Furthermore, in terms of this research implication to practice, this study acknowledges that analysts' responsibilities vary across SOCs and, as such, they may only perform a subset of the functions presented in the SOC-AAM. SOC managers and analysts can agree on the areas to measure. Also, in a SOC where certain functions are not provided, for example, some SOCs may not provide vulnerability management functions [30], the assessment criteria for those functions

can be dropped. On reflection, given that the SOC-AAM does not make a distinction between analyst tiers, its use could be more applicable in a non-hierarchical structure SOC, where all analysts are expected to have the same level of skills, performing the same functions and work independently [43, 56].

8.5 Research Limitations and Future Work

Although this study has a number strengths, there are some limitations. The first limitation is that it focuses only on task performance. The researcher acknowledges that individual work performance can be evaluated from other dimensions such as contextual performance, counterproductive work behaviour, and adaptive performance [59].

Future research could investigate how to measure an analyst's performance based on other dimensions. To the best of the researcher's knowledge, at the moment, there is no study that seeks to investigate how to measure an analyst's performance from the other human performance measure and dimensions reported in Section 4.6. Measuring performance from various dimensions from the researcher's perspective would be useful as it would offer SOC managers and stakeholders a more thorough, nuanced, and well-informed assessment of an analyst's overall performance. Indeed, by measuring performance from multiple angles, SOC managers will obtain a better insight into the overall performance of an analyst. Furthermore, measuring performance analysts from other dimensions would enable SOC managers to identify specific strengths and weaknesses.

Also, some participants commented that completing the SOC-AAM was time-consuming and advised integrating it with a ticketing system, such as Jira, to expedite the evaluation process. Future work could consider working with SOC system designers to automate and integrate the proposed assessment method into SOC tooling to assist the evaluation could be a potential solution to this constraint. Indeed, automating the assessment process would address the reported issue around the time-consuming nature of the

SOC-AAM. Moreover, automating the performance assessment would contribute to the mitigation of potential human errors associated with the existing manual process.

Another limitation of this study is the manager's random selection of a written report as part of the evaluation process. The manager may miss an incident report that is inadequately or poorly written. A solution to this problem could be a valuable contribution.

Finally, while the SOC-AAM was tested and evaluated in two SOCs, future work could consider extending the testing and evaluation to other industries and institutions.

8.6 Concluding statements

The research presented in this thesis addressed a long-standing research gap on SOCs that dates back to 2014 [54] and subsequently highlighted by other researchers [25, 39, 49, 53, 55, 56, 58], namely the lack of an adequate assessment method for analysts.

Using a DSR approach, this study proposed the SOC-AAM as a new formal method for measuring an analyst's performance in a systematic manner capturing the most important aspects of their work. Three iterations of the DSR process took place in this research, with each iteration creating an artefact that was subsequently evaluated by the SOC experts. This approach is consistent with the *"build"* and *"evaluate"* nature of design science research [229] and its iterative approach to constructing the artefacts [132].

This chapter has demonstrated that the research aims have been met and also described the research implications for both practice and research. Although some of the study participants reported during the evaluation phase that some analysts' tasks were not covered, the overall findings showed that the SOC-AAM covers the main functions of an analyst. Practitioners also commended on the usefulness of the guideline for assessing incident analysis and incident report. This discovery was a major goal and contribution

of this study. The results also revealed that the practitioners who participated in this study preferred to use the SOC-AAM for future evaluations of analysts' performance. The author hopes that SOCs looking for a way to measure the performance of analysts based on their task performance will find the SOC-AAM helpful in achieving this objective.

Bibliography

[1] S. M. Pedapudi and N. Vadlamani, "A comprehensive network security management in virtual private network environment," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE, 5 2022, pp. 1362–1367. [Online]. Available: https://ieeexplore.ieee.org/document/9793196/

[2] C. Zhong, T. Lin, P. Liu, J. Yen, and K. Chen, "A cyber security data triage operation retrieval system," *Computers & Security*, vol. 76, pp. 12–31, 7 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2018.02.011

[3] S. Yuan and C. Zou, "The security operations center based on correlation analysis," *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011*, pp. 334–337, 2011.

[4] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[5] G. Bendiab, K.-P. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: Security risks and mitigation," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*. ACM, 2020, pp. 1–8. [Online]. Available: https://doi.org/10.1145/3407023.3409312

[6] L. Aijaz, B. Aslam, and U. Khalid, "Security operations center - a need for an academic environment," in *2015 World Symposium on Computer Networks and Information Security (WSCNIS)*. IEEE, 2015, pp. 1–7.

[7] E. Falk, S. Repcek, B. Fiz, S. Hommes, R. State, and R. Sasnauskas, "VSOC - A virtual security operating center," *2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings*, vol. 8, pp. 1–6, 2017.

[8] Y. Creado and V. Ramteke, "Active cyber defence strategies and techniques for banks and financial institutions," *Journal of Financial Crime*, 5 2020. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/JFC-01-2020-0008/full/html

[9] K. Winterborn, "SOC maturity & capability," NCC Group, Tech. Rep., 2017. [Online]. Available: https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2017/ncc-group-whitepaper-soc-maturity-and-capability.pdf

[10] G. W. Chamiekara, M. I. Cooray, L. S. Wickramasinghe, Y. M. Koshila, K. Y. Abeywardhana, and A. N. Senarathna, "Autosoc: A low budget flexible security operations platform for enterprises and organizations," in *2017 National Information Technology Conference, NITC 2017*, 2017, pp. 100–105.

[11] Y. Creado and V. Ramteke, "Active cyber defence strategies and techniques for banks and financial institutions," *Journal of Financial Crime*, vol. 27, pp. 771–780, 5 2020.

[12] H. Xia and Y. Xu, "Design and research of safety test model based on advanced evasion techniques," in *Global Conference on Mechanics and Civil Engineering (GCMCE 2017)*, vol. 132. Atlantis Press, 2017, pp. 92–96.

[13] T. Arimatsu, Y. Yano, and Y. Takahashi, "Security operations center (soc) and security monitoring services to fight complexity and spread of cyber threats," *NEC Technical Journal*, vol. 12, no. 2, pp. 34–37, 2017.

[14] M. Collins, A. Hussain, and S. Schwab, "Towards an operations-aware experimentation methodology," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*. IEEE, 6 2022, pp. 384–393. [Online]. Available: https://ieeexplore.ieee.org/document/9799335/

[15] I. Taqafi, Y. Maleh, and K. Ouazzane, "A maturity capability framework for security operation center," *EDPACS*, vol. 67, pp. 21–38, 2023. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/07366981.2023.2159047

[16] M. Saraiva and N. Coelho, "Cybersoc implementation plan," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 6 2022, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9800819/

[17] A. Reisser, M. Vielberth, S. Fohringer, and G. Pernul, "Security operations center roles and skills: A comparison of theory and practice," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2022, pp. 316–327.

[18] D. Weissman and A. Jayasumana, "Integrating IoT monitoring for security operation center," in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*. Institute of Electrical and Electronics Engineers Inc., 6 2020, pp. 1–6.

[19] J. Suomalainen, J. Julku, A. Heikkinen, S. J. Rantala, and A. Yastrebova, "Security-driven prioritization for tactical mobile networks," *Journal of Information Security and Applications*, vol. 67, 6 2022.

[20] D. Shahjee and N. Ware, "Integrated network and security operation center: A systematic analysis," *IEEE Access*, vol. 10, pp. 27 881–27 898, 2022.

[21] S. Schinagl, K. Schoon, and R. Paans, "A framework for designing a security operations centre (soc)," in *2015 48th Hawaii International Conference on System Sciences*, vol. 2015-March. IEEE, 2015, pp. 2253–2262.

[22] NHS, "NHS to create a £20m soc and pen-testing operation," *Network Security*, vol. 2017, pp. 1–2, 12 2017.

[23] Research and Markets. (2019, 5) Soc as a service market - global forecast to 2024. [Online]. Available: https://www.globenewswire.com/news-release/2019/05/22/1840685/0/en/SOC-as-a-Service-Market-Global-Forecast-to-2024.html

[24] 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.

[25] S. Sundaramurthy, X. Ou, A. G. Bardas, J. Case, M. Wesch, J. Mchugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Symposium on Usable Privacy and Security*, 2015, pp. 347–359.

[26] C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, "Automate cybersecurity data triage by leveraging human analysts' cognitive process," in *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S*. IEEE, 2016, pp. 357–363.

[27] M. A. Majid and K. A. Z. Ariffi, "Success factors for cyber security operation center (soc) establishment," in *International Conference on Informatics, Engineering, Science and Technology*. European Alliance for Innovation (EAI), 2019.

[28] I. P. E. D. Nugraha, "International journal of current science research and review," *International Journal of Current Science Research and Review*, vol. 4, 2021. [Online]. Available: www.ijcsrr.org

[29] S. C. Sundaramurthy, J. McHugh, X. S. Ou, S. R. Rajagopalan, and M. Wesch, "An anthropological approach to studying csirts," *IEEE Security and Privacy*, vol. 12, pp. 52–60, 2014.

[30] P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers," in *2013 Information Security for South Africa*. IEEE, 8 2013, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/6641054/

[31] C. Onwubiko and A. Onwubiko, "Cyber kpi for return on security investment," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2019, pp. 1–8.

[32] M. Karyda, E. Mitrou, and G. Quirchmayr, "A framework for outsourcing is/it security services," *Information Management & Computer Security*, vol. 14, pp. 403–416, 10 2006. [Online]. Available: http://www.emeraldinsight.com/doi/10.1108/09685220610707421

[33] T. Shibahara, M. Akiyama, H. Kodera, K. Hato, D. Chiba, O. Soderstrom, D. Dalek, and M. Murata, "Cross-vendor knowledge transfer for managed security services with triplet network," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2019, pp. 59–69.

[34] R. Vaarandi and S. Mases, "How to build a soc on a budget," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2022, pp. 171–177.

[35] A. Shah, R. Ganesan, and S. Jajodia, "A methodology for ensuring fair allocation of csoc effort for alert investigation," *International Journal of Information Security*, vol. 18, pp. 1–20, 2018. [Online]. Available: https://doi.org/10.1007/s10207-018-0407-3

[36] Y. T. Dun, M. Faizal, A. Razak, M. F. Zolkipli, T. F. Bee, and A. Firdaus, "Grasp on next generation security operation centre (ngsoc): Comparative study," *Int. J. Nonlinear Anal. Appl*, vol. 12, pp. 2008–6822, 2021. [Online]. Available: http://dx.

[37] N. Miloslavskaya, A. Tolstoy, and S. Zapechnikov, "Taxonomy for unsecure big data processing in security operations centers," *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, pp. 154–159, 2016.

[38] C. Onwubiko and K. Ouazzane, "Cyber onboarding is 'broken'," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019)*. Institute of Electrical and Electronics Engineers Inc., 6 2019, pp. 1–13.

[39] S. A. Chamkar, Y. Maleh, and N. Gherabi, "The human factor capabilities in security operation centre (soc)," *The EDP Audit, Control, and Security Newsletter*, 2021. [Online]. Available: https://www.tandfonline.com/action/journalInformation?journalCode=uedp20

[40] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.chb.2015.01.039

[41] C. Acartürk, M. Ulubay, and E. Erdur, "Continuous improvement on maturity and capability of security operation centres," *IET Information Security*, vol. 15, no. 1, pp. 59–75, 2021.

[42] C. Feng, S. Wu, and N. Liu, "A user-centric machine learning framework for cyber security operations center," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 7 2017, pp. 173–175.

[43] S. A. Alharbi, "A qualitative study on security operations centers in saudi arabia: Challenges and research directions," *Journal of Theoretical and Applied Information Technology*, vol. 98, pp. 3972–3982, 2020.

[44] W. P. Aung, H. H. Lwin, and K. K. Lin, "Developing and analysis of cyber security models for security operation center in myanmar," in *2020 IEEE Conference on Computer Applications(ICCA)*. IEEE, 2 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9022821/

[45] C. Onwubiko and K. Ouazzane, "Challenges towards building an effective cyber security operations centre." *IJCSA*, vol. 4, pp. 11–39, 2019.

[46] L. Axon, J. R. C. Nurse, M. Goldsmith, and S. Creese, "A formalised approach to designing sonification systems for network-security monitoring," *International Journal on Advances in Security*, vol. 10, 2017. [Online]. Available: www.iaria.org

[47] C. Daniel, T. Gill, A. R. Hevner, and M. Mullarkey, "A deep neural network approach to tracing paths in cybersecurity investigations," in *IEEE International Conference on Data Mining Workshops, ICDMW*, vol. 2020-Novem. IEEE, 2020, pp. 472–479.

[48] T. Snoei. Network/security operations centre (soc). [Online]. Available: https://www.shutterstock.com/image-illustration/network-security-operations-center-soc-273294209

[49] 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.

[50] N. Alharbi, "A security operation center maturity model (soc-mm) in the context of newly emerging cyber threats," Ph.D. dissertation, The Claremont Graduate University, 2020.

[51] J. Goodall, W. Lutters, and A. Komlodi, "The work of intrusion detection: Rethinking the role of security analysts," *AMCIS 2004 Proceedings*, pp. 1421–1427, 2004.

[52] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in *2015*

International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, 6 2015, pp. 1–10. [Online]. Available: http://ieeexplore.ieee.org/document/7166125/

[53] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *Journal of Information Security and Applications*, vol. 48, p. 102352, 10 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2214212618307804

[54] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," in *Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW '14*. ACM, 2014, pp. 43–50. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663887.2663904

[55] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Towards a framework for measuring the performance of a security operations center analyst," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 2020, pp. 1–8.

[56] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched socs: A qualitative study on security operations center issues," *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pp. 1955–1970, 2019.

[57] 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.

[58] S. C. Sundaramurthy, M. Wesch, X. Ou, J. McHugh, S. R. Rajagopalan, and A. G. Bardas, "Humans are dynamic-our tools should be too," *IEEE Internet Computing*, vol. 21, pp. 40–46, 5 2017.

[59] L. Koopmans, "Measuring individual performance," Ph.D. dissertation, Tufts Medical Center, 2014.

[60] R. Islam and S. bin Mohd Rasad, "Employee performance evaluation by ahp: A case study," *Asia Pacific Management Review*, vol. 11, p. 16, 2006.

[61] T. A. O'Connell and Y. Y. Choong, "Metrics for measuring human interaction with interactive visualizations for information analysis," in *Conference on Human Factors in Computing Systems - Proceedings*. ACM, 2008, pp. 1493–1496.

[62] P. Farrugia, B. A. Petrisor, F. Farrokhyar, and M. Bhandari, "Research questions, hypotheses and objectives," *Canadian Journal of Surgery*, vol. 53, p. 278, 2010. [Online]. Available: /pmc/articles/PMC2912019/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2912019/

[63] J. Dudovskiy. Formulating research aims and objectives - research-methodology. [Online]. Available: https://research-methodology.net/research-methodology/research-aims-and-objectives/

[64] R. Kumar, *Research methodology: a step-by-step guide for beginners*, 5th ed. Sage publications Ltd, 2019.

[65] J. L. Hull, "Analyst burnout in the cyber security operations centre - csoc: A phenomenological study," Ph.D. dissertation, Colorado Technical University, 2017.

[66] G. M. Sullivan and J. Sargeant, "Qualities of qualitative research: Part i," *Journal of Graduate Medical Education*, pp. 449–452, 2011. [Online]. Available: http://dx.doi.org/10.4300/JGME-D-11-00221.1

[67] C. Clay. (2018) Difference between proposition & hypothesis. [Online]. Available: https://sciencing.com/difference-between-proposition-hypothesis-12749814.html

[68] T. Saaty, *Decision making for leaders: the analytical hierarchy process for decisions in a complex world*. RWS Publications, 2008.

[69] 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. 102959, 2023.

[70] C. S. 2020. Advancing a multidisciplinary approach to cyber security. [Online]. Available: https://www.c-mric.com/

[71] 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 2018*. IEEE, 2018, pp. 1–6.

[72] C. Onwubiko and K. Ouazzane, "Soter: A playbook for cyber security incident management," *IEEE Transaction of Engineering and Management*, pp. 1–22, 2019.

[73] M. Dietz, M. Vielberth, and G. Pernul, "Integrating digital twin security simulations in the security operations center," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–9.

[74] IDRBT, "Handbook on information security operations center," Institute for Development and Research in Banking Technology, Tech. Rep., 2017. [Online]. Available: http://www.idrbt.ac.in/assets/publications/BestPractices/ISOC.pdf

[75] J. M. Brown, S. Greenspan, and R. Biddle, "Incident response teams in it operations centers: the t-tocs model of team functionality," *Cognition, Technology & Work*, vol. 18, pp. 695–716, 2016. [Online]. Available: https://link-springer-com.abc.cardiff.ac.uk/content/pdf/10.1007/s10111-016-0374-2.pdf

[76] N. Miloslavskaya, "Information security management in socs and sics," *Journal of Intelligent & Fuzzy Systems*, vol. 35, pp. 2637–2647, 2018. [Online]. Available: https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs169615

[77] T. Sander and J. Hailpern, "UX aspects of threat information sharing platforms," *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS '15*, pp. 51–59, 2015. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2808128.2808136

[78] R. D. Mooi and R. A. Botha, "A management model for building a computer security incident response capability," *SAIEE Africa Research Journal*, vol. 107, pp. 78–91, 2016.

[79] B. P. Hámornik and C. Krasznay, "A team-level perspective of human factors in cyber security: security operations centers," in *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on*

Human Factors in Cybersecurity, July 17- 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8. Springer, 2018, pp. 224–236.

[80] C. C. L. Paul, "Human-centered study of a network operations center: Experience report and lessons learned," in *Proceedings of the ACM Workshop on Security Information Workers*, 2014, pp. 39–42. [Online]. Available: http://dl.acm.org/citation.cfm?id=2663899http://dx.doi.org/10.1145/2663887.2663899

[81] C. Zimmerman, *Cybersecurity Operations Center*. The MITRE Corporation, 2014.

[82] M. Libis, C. Wardana, and A. Widjajarto, "The development of information system security operation centre (soc): Case study of auto repair company," in *2020 6th International Conference on Interactive Digital Media (ICIDM)*. IEEE, 2020, pp. 1–8.

[83] Hewlett-Packard, "5g/soc: Soc generations -hp esp security intelligence and operations consulting services - business white paper," Hewlett-Packard, Tech. Rep., 2013.

[84] T. Security. (2017) The rise of next generation security operation center (ng-soc). [Online]. Available: https://medium.com/taslet-security/the-rise-of-next-generation-security-operation-center-ng-soc-266d0522681b

[85] M. D. E. Corporation, "Industry guidance for next generation security operating centre," MDEC, Tech. Rep. [Online]. Available: https://mdec.my/assets/pdf/Industry-Guidance-for-Next-Generation-Managed-Security-Operating-Centre.pdf

[86] G. Kaur and A. H. Lashkari, "An introduction to security operations," in *Advances in Cybersecurity Management*. Springer International Publishing, 2021, pp. 463–481. [Online]. Available: https://link.springer.com/10.1007/978-3-030-71381-2_21

[87] A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "Adaptive reallocation of cybersecurity analysts to sensors for balancing risk between sensors," *Service Oriented Computing and Applications*, vol. 12, pp. 123–135, 2018. [Online]. Available: https://doi.org/10.1007/s11761-018-0235-3

[88] T. Kwon, J. suk Song, S. Choi, Y. Lee, and J. Park, "Visnu: A novel visualization methodology of security events optimized for a centralized soc," *2018 13th Asia Joint Conference on Information Security (AsiaJCIS)*, pp. 1–7, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8453754/

[89] A. Shah, R. Ganesan, S. Jajodia, and C. A. Hasan, "An outsourcing model for alert analysis in a cybersecurity operations center," *ACM Transactions on the Web*, vol. 14, pp. 1–22, 1 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3372498

[90] N. C. S. Centre, "The cyber threat to uk business," National Cyber Security Centre, Tech. Rep., 2018. [Online]. Available: http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file

[91] A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "Understanding trade-offs between throughput, quality, and cost of alert analysis in a csoc," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 1155–1170, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8470145/

[92] F. D. János and N. H. P. Dai, "Security concerns towards security operations centers," *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, pp. 000 273–000 278, 2018.

[93] A. E. Thomas, *Security operations center : analyst guide*. CreateSpace, 2016.

[94] L. Jefferies. (2017) What makes a security operations centre effective? [Online]. Available: https://www.csiltd.co.uk/makes-security-operations-centre-effective/

[95] SANS, "Roadmap to creating a world-class security operations center," SANS Institute, Tech. Rep., 2015. [Online]. Available: https://www.rsa.com/content/dam/en/infographic/rsa-sans-roadmap-to-creating-a-world-class-soc.pdf

[96] P. Mcevatt, "Advanced threat centre and future of security monitoring," *Fujitsu Scientific & Technical Journal*, vol. 55, pp. 16–22, 2019.

[97] D. Crémilleux, C. Bidan, F. Majorczyk, and N. Prigent, "Enhancing collaboration between security analysts in security operations centers," in *Risks and Security of Internet and Systems: 13th International Conference, CRiSIS 2018, Arcachon, France, October 16–18, 2018, Revised Selected Papers 13*. Springer, 2019, pp. 136–142.

[98] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo, "Training the maritime security operations centre teams," in *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*. IEEE, 2022, pp. 388–393.

[99] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "Cybersecurity incident response in organizations: An exploratory case study and process model of situation awareness," *Computers & Security*, vol. 101, pp. 102–122, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2020.102122

[100] Ernest and Y. (EY), "Security operations centers - helping you get ahead of cybercrime," Ernest & Young, Tech. Rep., 2014. [Online]. Available: www.ey.com/GISS2014.

[101] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The human factor of information security: Unintentional damage perspective," *Procedia - Social and Behavioral Sciences*, vol. 147, pp. 424–428, 2014. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1877042814040440

[102] J. Mcclain, A. Silva, G. Emmanuel, B. Anderson, K. Nauer, R. Abbott, and C. Forsythe, "Human performance factors in cyber security forensic analysis," *Procedia Manufacturing*, vol. 3, pp. 5301–5307, 2015. [Online]. Available: www.sciencedirect.com

[103] Z. Naz. (2023, 9) Soc analyst: Job description, roles & responsibilities. [Online]. Available: https://www.knowledgehut.com/blog/security/soc-analyst

[104] Intellipaat. (2023, 7) Soc analyst - what is a soc analyst, and what do they do?

[105] Cisco Inc. (2023) Launch your career in cybersecurity operations with cyberops associate. [Online]. Available: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html

[106] EC-Council. (2023) Ec-council learning: Cybersecurity course library. [Online]. Available: https://iclass.eccouncil.org/our-courses/

[107] S. Coutinho, A. Bollen, C. Weil, C. Sheerin, D. Silvera, S. Donaldson, and J. Rosborough, "Cyber security skills in the uk labour market 2023 findings report," Department for Science, Information & Technology, Tech. Rep., 2023.

[108] O. Santos, R. Taylor, and J. Mlodzianowski, *CompTIA Security+ SY0-601 Cert Guide*. Pearson IT Certification, 2021.

[109] S. Furnell, "The cybersecurity workforce and skills," *Computers & Security*, vol. 100, 1 2021.

[110] S. Furnell, P. Fischer, and A. Finch, "Can't get the staff? the growing need for cyber-security skills," *Computer Fraud & Security*, 2017.

[111] M. Nakayama and N. G. Sutcliffe, "It skills portfolio research in sigcpr proceedings: Analysis, synthesis and proposals," in *SIGCPR '01: Proceedings of the 2001 ACM SIGCPR conference on Computer personnel research*, 2001.

[112] C. Beaumont and P. Hartley, "The cyber security knowledge exchange: Working with employers to produce authentic pbl scenarios and enhance employability," *Transactions on Edutainment XV*, pp. 209–228, 2019.

[113] C. Swarnalatha and T. Prasanna, "Leveraging employee engagement for competitive advantage: Strategic role of hr," *Review of HRM*, vol. 2, p. 139, 2013.

[114] I. Kilaz, A. Onder, and M. Yanik, "Manpower planning and management in cyber defense," in *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*, 2014, p. 116.

[115] T. Caldwell, "Plugging the cyber-security skills gap," *Computer Fraud & Security*, vol. 2013, no. 7, pp. 5–10, 2013.

[116] T. De Zan, "Mind the gap: the cyber security skills shortage and public policy interventions," 2019.

[117] G. P. Tadda, "Measuring performance of cyber situation awareness systems," in *2008 11th International Conference on Information Fusion*. IEEE, 2008, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4632229

[118] M. Vielberth, "Security operations center (soc)," University of Regensburg, Tech. Rep., 2021. [Online]. Available: https://doi.org/10.1007/978-3-642-27739-9_1680-1

[119] T. Tafazzoli and H. G. Garakani, "Security operation center implementation on openstack," in *2016 8th International Symposium on Telecommunications, IST 2016*. Institute of Electrical and Electronics Engineers Inc., 3 2016, pp. 766–770.

[120] M. Evans, Y. He, L. Maglaras, and H. Janicke, "Heart-is: A novel technique for evaluating human error-related information security incidents," *Computers & Security*, vol. 80, pp. 74–89, 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404818301615

[121] P. P. Texel, "Measure , metric , and indicator :," in *2013 Proceedings of IEEE Southeastcon*. IEEE, 2013, pp. 1–5.

[122] P. J. Houngbo and J. T. Hounsou, "Measuring information security: understanding and selecting appropriate metrics," *International Journal of Computer Science and Security (IJCSS)*, vol. 9, no. 2, p. 108, 2015.

[123] R. L. Thomas and D. Uminsky, "Reliance on metrics is a fundamental challenge for ai," *Patterns*, vol. 3, p. 100476, 2022. [Online]. Available: https://doi.org/10.1016/j.patter.2022.100476

[124] R. K. A. Ahmed, "Overview of Security Metrics," *Software Engineering*, vol. 4, no. 4, pp. 59–64, 2016.

[125] J. Scholtz and M. P. Steves, "A framework for real-world software system evaluations," in *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. ACM, 2004, pp. 600–603.

[126] S. C. Buttigieg, A. Pace, and C. Rathert, "Hospital performance dashboards: a literature review," *Journal of health organization and management*, 2017. [Online]. Available: www.emeraldinsight.com/1477-7266.htm

[127] J. G. Voeller, P. E. Black, K. Scarfone, and M. Souppaya, "Cyber security metrics and measures," National Institute of Science and Technology, Tech. Rep., 2008.

[128] L. Hayden, *IT Security Metrics : A Practical Framework for Measuring Security and Protecting Data*. McGraw Hill, 2010.

[129] R. S. Kaplan, *Measuring performance: expert solutions to everyday challenges*. Harvard Business Press, 2009.

[130] T. Sadamatsu, Y. Yoneyama, and K. Yajima, "Practice within fujitsu of security operations center: Operation and security dashboard," Fujitsu, Tech. Rep., 2016. [Online]. Available: https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-3/paper08.pdf

[131] P. Offermann, O. Levina, M. Schönherr, and U. Bub, "Outline of a design science research process," in *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, 2009, pp. 1–11.

[132] V. Vaishnavi and B. Kuechler, "Design science research in information systems overview of design science research," in *Ais*, V. Vaishnavi, B. Kuechler, and S. Petter, Eds., 2004, p. 45. [Online]. Available: http://www.desrist.org/design-research-in-information-systems/

[133] S. Weber, "Design science research: Paradigm or approach?" in *Americas Conference on Information Systems (AMCIS) 2010 Proceedings*, 2010, p. 214. [Online]. Available: http://aisel.aisnet.org/amcis2010http://aisel.aisnet.org/amcis2010/214

[134] D. Kehily and J. Underwood, "Design science: Choosing an appropriate methodology for research in bim," in *CitA BIM Gathering*. CITA, 2015. [Online]. Available: http://usir.salford.ac.uk/id/eprint/38522/

[135] P. Jarvinen, "Research questions guiding selection of an appropriate research method," in *Proceedings of the European Conference on Information Systems*, vol. 3, 2000, pp. 124–131. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.144.2055&rep=rep1&type=pdf%5Cnhttp://60.88.dyn.lse.ac.uk/asp/aspecis/20000024.pdf

[136] P. Adu, *A step-by-step guide to qualitative data coding*, 1st ed. Routledge, 2019.

[137] C. Dawson, *Introduction to research methods: a practical guide for anyone undertaking a research project*, 5th ed. Robinson, 2019.

[138] P. Johannesson and E. Perjons, *An introduction to design science*. Springer International Publishing, 2014.

[139] A. R. Hevner and S. Gregor, "Positioning and presenting design science: Types of knowledge in design science research," *MIS Quarterly*, vol. 37, pp. 337–355, 2013.

[140] R. W. Gregory, "Design science research and the grounded theory method: Characteristics, differences, and complementary uses," *18th European Conference on Information Systems*, 2010.

[141] J. E. V. Aken, "Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules," *Journal of management studies*, vol. 41, pp. 219–246, 2004. [Online]. Available: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-6486.2004.00430.x

[142] J. Iivari and J. R. Venable, "Action research and design science research - seemingly similar but decisively dissimilar," *Association for Information Systems AIS Electronic Library*, 2009. [Online]. Available: http://aisel.aisnet.org/ecis2009/73

[143] N. Papas, R. M. O'Keefe, and P. Seltsikas, "The action research vs design science debate: reflections from an intervention in egovernment," *European Journal of Information Systems*, vol. 21, pp. 147–159, 2012. [Online]. Available: https://www.tandfonline.com/action/journalInformation?journalCode=tjis20

[144] A. R. Hevner, R. Sudhan, M. T. Salvatore, and P. Jinsoo, "Design science in information systems research," *MIS Quarterly*, vol. 42, pp. 5020–5028, 2004.

[145] R. Baskerville, "What design science is not," *European Journal of Information Systems*, vol. 17, pp. 441–443, 2008. [Online]. Available: www.palgrave-journals.com/ejis

[146] E. Costa, A. L. Soares, and J. P. D. Sousa, "Situating case studies within the design science research paradigm: An instantiation for collaborative networks," in *17th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2016, Porto, Portugal, October 3-5, 2016, Proceedings*. Springer, Cham, 2016, pp. 531–544. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-3-319-45390-3_45.pdf

[147] P. Lif and T. Sommestad, "Human factors related to the performance of intrusion detection operators," in *HAISA*, 2015, pp. 265–275. [Online]. Available: https://pdfs.semanticscholar.org/9ec5/14d9705aa4e85356fb5385f04932e68cdb6c.pdf

[148] N. King, "Qualitative organizational research: Core methods and current challenges - google books," in *Qualitative Organizational Research: Core Methods and Current Challenges*. Sage Publications Ltd, 2012, p. 426â50.

[149] A. R. Henver, "A three cycle view of design science research," *Scandinavian Journal of Information Systems*, vol. 19, 2007. [Online]. Available: http://aisel.aisnet.org/sjis/vol19/iss2/4

[150] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. Sage Publication, Inc., 2018.

[151] T. J. Gordon, "The delphi method in futures research methodology-v3.0," *The Millenium Project*, 2011.

[152] D. L. Moody, "The method evaluation model: A theoretical model for validating information systems design methods," in *European Conference on Information Systems (ECIS)*, 2003. [Online]. Available: http://aisel.aisnet.org/ecis2003/79

[153] L. Y. Conrad and V. M. Tucker, "Making it tangible: hybrid card sorting within qualitative interviews," *Journal of Documentation*, 2019. [Online]. Available: www.usabilitest.

[154] O. Doody and M. Noonan, "Preparing and conducting interviews to collect data," *Nurse Researcher*, vol. 20, pp. 28–32, 2013.

[155] S. Rose, N. Spinks, and A. I. Canhoto, *Management Research: Applying the Principles*. Routledge, 2015.

[156] C. B. Meyer, "A case in case study methodology," *Field Methods*, vol. 13, pp. 329–352, 11 2001. [Online]. Available: http://journals.sagepub.com/doi/10.1177/1525822X0101300402

[157] M. Denscombe, *The good research guide: for small-scale social research projects*, 6th ed. Open University Press, 2017.

[158] E. O. Ahmed, "The ottoman perception in process: Turkey social studies textbook analysis," *Educational Research and Reviews*, vol. 15, pp. 129–137, 2020.

[159] S. Stein, Y. Lauer, and M. E. Kharbili, "Using template analysis as background reading technique forrequirements elicitation," in *Software Engineering*, 2009. [Online]. Available: http://www.ip-super.org/

[160] M. Othman and S. Ghanbari, "A priority based job scheduling algorithm in cloud computing," *Procedia Engineering*, vol. 50, pp. 778–785, 2012. [Online]. Available: www.elsevier.com/locate/procedia

[161] J. Benítez, X. Delgado-Galván, J. A. Gutiérrez, and J. Izquierdo, "Balancing consistency and expert judgment in ahp," *Mathematical and Computer Modelling*, vol. 54, no. 7-8, pp. 1785–1790, 2011.

[162] N. Badie and A. H. Lashkari, "A new evaluation criteria for effective security awareness in computer risk management based on ahp," *Journal of Basic and Applied Scientific Research*, vol. 2, pp. 9331–9347, 2012.

[163] H. M. Fahmy, "Reliability evaluation in distributed computing environments using the ahp," *Computer Networks*, vol. 36, pp. 597–615, 8 2001.

[164] L. Bodin and E. Epstein, "Who's on first-with probability 0.4," *Computers and Operations Research*, vol. 27, pp. 205–215, 3 2000.

[165] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, pp. 68–77, 2005.

[166] T. Saaty, "How to make a decision: The analytic hierachy process," *European Journal of Operational Research*, vol. 48, pp. 9–26, 1990.

[167] T. L. Saaty, *The analytic hierarchy process: planning, priority setting, resource allocation*. McGraw-Hill International Book Co, 1980.

[168] A. Shahin and M. A. Mahbod, "Prioritization of key performance indicators: An integration of analytical hierarchy process and goal setting," *International Journal of Productivity and Performance Management*, vol. 56, 2007. [Online]. Available: www.emeraldinsight.com/1741-0401.htm

[169] M. Turoff and H. A. Linstone, "The delphi method: Techniques and applications, 2002," 2018.

[170] A. M. Arof, "The application of a combined delphi-ahp method in maritime transport research-a review," *Asian Social Science*, vol. 11, pp. 73–82, 2015.

[171] X. Gan, J. Duanmu, and H. Wang, "Delphi analysis method and its application in qualitative prediction of aircraft collision unsafe event for air traffic control," in *International Conference on Intelligent Systems Research and Mechatronics Engineering*. Atlantis Press, 2015, pp. 1472–1475.

[172] M. Taleai and A. Mansourian, "Using delphi-ahp method to survey major factors causing urban plan implementation failure," *Journal of Applied Sciences*, vol. 8, pp. 2746–2751, 2008.

[173] J. Dudovskiy. (2019) Sampling in primary data collection. [Online]. Available: https://research-methodology.net/sampling-in-primary-data-collection/

[174] E. Ogbeifun, J. Agwa-Ejon, C. Mbohwa, and J. H. Pretorius, "The delphi technique: A credible research methodology," *Proceedings of the International Conference on Industrial Engineering and Operations Management*, vol. 8-10 March, pp. 2004–2009, 2016.

[175] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 77–101, 2006. [Online]. Available: https://www.tandfonline.com/action/journalInformation?journalCode=uqrp20

[176] J. Green and N. Thorogood, *Qualitative Methods for Health Research*, 4th ed. Sage Publications, 2018.

[177] R. Knight and J. R. Nurse, "A framework for effective corporate communication after cyber security incidents," *Computers & Security*, vol. 99, p. 102036, 2020.

[178] J. Brooks, S. Mccluskey, E. Turley, and N. King, "The utility of template analysis in qualitative psychology research," *Qualitative Research in Psychology*, vol. 12, pp. 202–222, 2015.

[179] S. C. Sundaramurthy, J. Mchugh, X. Ou, M. Wesch, A. G. Bardas, J. Mchugh, and S. R. Rajagopalan, "Turning contradictions into innovations or : How we learned to stop whining and improve security operations." in *the Symposium On Usable Privacy and Security (SOUPS)*. USENIX, 2016, pp. 237–251.

[180] H. Alshenqeeti, "Interviewing as a data collection method: A critical review," *English Linguistics Research*, vol. 3, pp. 39–45, 2014. [Online]. Available: http://www.sciedu.ca/journal/index.php/elr/article/view/4081

[181] B. S. Cypress, "Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations," *Dimensions of Critical Care Nursing*, vol. 36, pp. 253–263, 2017.

[182] J. W. Creswell and J. D. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*, 5th ed. Sage Publications, 2018.

[183] D. R. Thomas, "Feedback from research participants: are member checks useful in qualitative research?" *Qualitative Research in Psychology*, vol. 14, pp. 23–41, 1 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/14780887.2016.1219435

[184] J. A. Carlson, "Avoiding traps in member checking," *The Qualitative Report*, vol. 15, pp. 1102–1113, 2010. [Online]. Available: https://nsuworks.nova.edu/tqr/vol15/iss5/4

[185] M. Fekete and I. Rozenberg, "The practical model of employee performance evaluation," *Management, Knowledge & Learning*, pp. 141–149, 2014.

[186] A. Gunasekaran, C. Patel, and E. Tirtiroglu, "Performance measures and metrics in a supply chain environment," *International Journal of Operations & Production Management*, vol. 21, pp. 71–87, 1 2001. [Online]. Available: https://www.emeraldinsight.com/doi/10.1108/01443570110358468

[187] L. Koopmans, C. M. Bernaards, V. H. Hildebrandt, W. B. Schaufeli, C. W. D. V. Henrica, and A. J. V. D. Beek, "Conceptual frameworks of individual work performance: A systematic review," *Journal of Occupational and Environmental Medicine*, vol. 53, pp. 856–866, 2011. [Online]. Available: http://dx.doi.org/10.1097/JOM.0b013e318226a763

[188] S. M. Taj and A. Kumaravel, "Measuring employee performance key indicators by fuzzy petri nets," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 9, pp. 485–490, 2015.

[189] K. Brotby and G. Hinson, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. CRC Press, 2013. [Online]. Available: https://books.google.com/books?id=4DfOBQAAQBAJ&pgis=1

[190] M. B. Fall, "Strategies business managers use to improve employee performance," Ph.D. dissertation, Walden University, 2020.

[191] R. L. S. Silva and F. W. Neiva, "Systematic literature review in computer science-a practical guide," Federal University of Juiz de Fora, Tech. Rep., 2016. [Online]. Available: https://www.researchgate.net/publication/320704338

[192] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Software Engineering Group School of Computer Science and Mathematics Keele, Tech. Rep., 2007. [Online]. Available: https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs169615

[193] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, vol. 55, pp. 2049–2075, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.infsof.2013.07.010

[194] University of Liverpool. (2018) Which are the best databases for computer science? - library help. [Online]. Available: https://libanswers.liverpool.ac.uk/faq/49363

[195] W. Jansen, *Directions in security metrics research*. Diane Publishing, 2010. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7564.pdf

[196] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Pearson Education, Inc., 2007.

[197] L. Koopmans, C. Bernaards, V. Hildebrandt, S. V. Buuren, A. J. V. D. Beek, and H. C. de Vet, "Development of an individual work performance questionnaire," *International Journal of Productivity and Performance Management*, vol. 62, pp. 6–28, 2012.

[198] E. Chickowski. (2015) Dark reading - 10 ways to measure IT security program effectiveness. [Online]. Avail-

able: https://www.darkreading.com/analytics/10-ways-to-measure-it-security-program-effectiveness/d/d-id/1319494?print=yes{&}image_number=1

[199] C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, "Learning from experts' expereince:toward automated cyber security data triage," *IEEE Systems Journal*, vol. i, pp. 1–12, 2018.

[200] K. Kuutti, "Activity theory as a potential framework for human-computer interaction research," in *Context and Consciousness: Activity Theory and Human-Computer Interaction*, B. A. Nardi, Ed. MIT Press, 1996, p. 400.

[201] P. Zhang, I. Benbasat, J. Carey, F. Davis, D. Galletta, and D. Strong, "Human-computer interaction research in the mis discipline," *Former Departments, Centers, Institutes and Projects*, vol. 9, pp. 334–355, 2002. [Online]. Available: http://sighci.org/amcis02/amcis02_panel/CAIS02_Zhang_etal_Journal.pdf

[202] A.-L. Fayard and W. E. Mackay, "Hci, natural science and design: A framework for triangulation across disciplines," in *Symposium on Designing Interactive Systems: Proceedings of the 2 nd conference on Designing interactive systems: processes, practices, methods, and techniques*, 1997, pp. 223–234. [Online]. Available: https://www.researchgate.net/publication/2644577

[203] J. Xu, S. Anders, A. Pruttianan, D. France, N. Lau, J. A. Adams, and M. B. Weinger, "Human performance measures for the evaluation of process control human-system interfaces in high-fidelity simulations," *Applied Ergonomics*, vol. 73, pp. 151–165, 2018. [Online]. Available: https://doi.org/10.1016/j.apergo.2018.06.008

[204] C. Onwubiko, "Understanding cyber situation awareness," *IJCSA*, vol. 1, pp. 11–30, 2016. [Online]. Available: http://www.c-mric.com/wp-content/uploads/2017/10/article1.pdf

[205] M. R. Endsley, "Measurement of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, pp. 65–84, 2006.

[206] E. Dafikpaku, "The strategic implication of enterprise risk management (erm): A framework," in *ERM Symposium*, vol. 48. Society of Actuaries, 2011.

[207] S. Mansfield-Devine, "Creating security operations centres that work," *Network Security*, vol. 2016, pp. 15–18, 2016. [Online]. Available: http://osdelivers.blackducksoftware.http://dx.doi.org/10.1016/S1353-4858(16)30049-6

[208] M. A. Majid, K. Akram, and Z. Ariffin, "Model for successful development and implementation of cyber security operations centre (soc)," *PLoS ONE*, vol. 16, pp. 1–24, 2021. [Online]. Available: http://dx.doi.org/10.1371/journal.pone.0260157

[209] CESG, "GPG 13 - Protective Monitoring for HMG ICT - Issue 1.7 October 2012," CESG-Communications Electronics Security Group, Tech. Rep., 2012. [Online]. Available: https://www.ncsc.gov.uk/guidance/protective-monitoring-hmg-ict-systems-gpg-13

[210] D. Botta, R. Werlinger, A. Gagne, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding it security professionals and their tools," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2008, p. 100.

[211] SANS Institute, *SEC504: Hacker Techniques, Exploits, and Incident Handling*. The SANS Institute, 2018.

[212] A. D'Amico and K. Whitley, "The real work of computer network defense analysts," in *VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security*. springer berlin, 2008, pp. 19–37.

[213] R. Graf and R. King, "Cyber threat information classification and life cycle management using smart contracts," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pp. 304–311, 2018. [Online]. Available: http://caesair.ait.ac.at

[214] D. L. Deadrick and D. G. Gardner, "Performance distributions : Measuring employee performance using total quality management principles," *Journal of Quality Management*, vol. 4, pp. 225–241, 1999.

[215] P. I. Fusch and L. R. Ness, "Are we there yet? data saturation in qualitative research," *The Qualitative Report*, vol. 20, pp. 1408–1416, 2015. [Online]. Available: http://scholarworks.waldenu.edu/sm_pubs

[216] J. M. Ahrend, M. Jirotka, and K. Jones, "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence

knowledge," in *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016*. IEEE, 2016, pp. 1–10.

[217] K. Chałubińska-Jentkiewicz, F. Radoniewicz, and T. Zieliński, *Cybersecurity in Poland: Legal Aspects*. Springer Nature, 2022.

[218] N. Miloslavskaya, "Security operations centers for information security incident management," in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 2016, pp. 131–138.

[219] D. P. Biros and T. Eppich, "Human element key to intrusion detection," *Signal*, 2001. [Online]. Available: https://www.afcea.org/content/human-element-key-intrusion-detection

[220] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 49, pp. 229–233, 2005. [Online]. Available: http://journals.sagepub.com/doi/10.1177/154193120504900304

[221] G. Odu, "Weighting methods for multi-criteria decision making technique," *Journal of Applied Sciences and Environmental Management*, vol. 23, p. 1449, 2019.

[222] R. V. Vargas, "Using the analytic hierarchy process (ahp) to select and prioritize projects in a portfolio," in *PMI Global Congress*, vol. 32. PA:Project Management Institute, 2010, pp. 1–22.

[223] S. S. Sidhu, K. Singh, and I. S. Ahuja, "Ranking of implementation dimensions for maintenance practices in northern indian smes using integrated ahp-topsis approach," *Journal of Small Business And Entrepreneurship*, pp. 1–20, 2020. [Online]. Available: https://www.tandfonline.com/action/journalInformation?journalCode=rsbe20

[224] A. Ishizaka and A. Labib, "Review of the main developments in the analytic hierarchy process," *Expert Systems with Applications*, vol. 38, pp. 14 336–14 345, 2011.

[225] F. D. Felice and A. Petrillo, "Absolute measurement with analytic hierarchy process: A case study for italian racecourse," *International Journal of Applied Decision Sciences*, vol. 6, pp. 209–227, 2013.

[226] T. L. Saaty, "Decision-making with the ahp: Why is the principal eigenvector necessary," *European Journal of Operational Research*, vol. 145, pp. 85–91, 2003.

[227] M. El-Mekawy, L. Rusu, and E. Perjons, "An evaluation framework for comparing business-it alignment models: A tool for supporting collaborative learning in organizations," *Computers in Human Behavior*, vol. 51, pp. 1229–1247, 2015.

[228] K. Peffers, T. Tuunanen, C. Gengler, M. Rossi, W. Hui, V. V., and J. Bragge, "The design science research process: A model for producing and presenting information systems research," in *First International Conference on Design Science Research in Information Systems and Technology*, 2006, pp. 83–106.

[229] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, pp. 251–266, 1995.

[230] K. Peffers, M. Rothenberger, T. Tuunanen, and R. Vaezi, "Design science research evaluation," in *Design Science Research in Information Systems. Advances in Theory and Practice. DESRIST 2012. Lecture Notes in Computer Science*, K. Peffers, M. Rothenberger, and B. Kuechler, Eds. Springer, 2012, pp. 398–410. [Online]. Available: http://link.springer.com/10.1007/978-3-642-29863-9_29

[231] J. Aronson, "The qualitative report a pragmatic view of thematic analysis," *The Qualitative Report*, vol. 2, pp. 1–3, 1995. [Online]. Available: https://nsuworks.nova.edu/tqr/vol2/iss1/3

[232] P. Bellström and C. Kop, "Towards a framework for schema quality in the schema integration process," *actice of*, p. 60, 2012.

[233] E. Paintsil, "Taxonomy of security risk assessment approaches for researchers," in *Proceedings of the 2012 4th International Conference on Computational Aspects of Social Networks, CASoN 2012*. IEEE, 2012, pp. 257–262.

[234] Q. Albluwi, "Framework for performance evaluation of computer security incident response capabilities," Ph.D. dissertation, University of Rhode Island, 2017.

[235] E. Bell, A. Bryman, and B. Harley, *Business Research Methods*, 5th ed. Oxford University Press, 2018.

[236] J. A. Zachman, "Concepts of the framework for enterprise architecture," *Zachman International*, 1996.

[237] C. Onwubiko, "Focusing on the recovery aspects of cyber resilience," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, 2020.

[238] E. Paintsil, "Evaluation of privacy and security risks analysis construct for identity management systems," *IEEE Systems Journal*, vol. 7, pp. 189–198, 2012.

[239] J. Recker, "Understanding process modeling grammer continuance: A study of the consequences of representational capabilities," Ph.D. dissertation, Queensland University of Technology, 2008.

[240] A. Gunasekaran, C. Patel, and R. E. McGaughey, "A framework for supply chain performance measurement," *International Journal of Production Economics*, vol. 87, pp. 333–347, 2004.

[241] T. Chen, Y. Chen, H. Guo, and J. Luo, "When e-commerce meets social media: Identifying business on wechat moment using bilateral-attention lstm," in *The Web Conference 2018 - Companion of the World Wide Web Conference, WWW 2018*. Association for Computing Machinery, Inc, 4 2018, pp. 343–350.

[242] F. Paz, F. A. Paz, and J. A. Pow-Sang, "Experimental case study of new usability heuristics," in *Design, User Experience, and Usability: Design Discourse: 4th International Conference, DUXU 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2–7, 2015, Proceedings, Part I*. Springer, 2015, pp. 212–223.

[243] F. Paz, D. Villanueva, C. Rusu, S. Roncagliolo, and J. A. Pow-Sang, "Experimental evaluation of usability heuristics," *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013*, pp. 119–126, 2013.

[244] J. Recker, M. Rosemann, and W. V. der Aalst, "On the user perception of configurable reference process models - initial insights," *ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems*, p. 66, 2005.

[245] N. Condori-Fernandez and O. Pastor, "Re-assessing the intention to use a measurement procedure based on cosmic-ffp," in *International Conference on Software Process and Product Measurement*, 2006, p. 63.

[246] J. A. Pow-Sang, R. Imbert, and A. M. Moreno, "A replicated experiment with undergraduate students to evaluate the applicability of a use case precedence diagram based approach in software projects," *Communications in Computer and Information Science*, vol. 257 CCIS, pp. 169–179, 2011. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-27207-3_17

[247] S. Abrahão, G. Poels, and E. Insfran, "A replicated study on the evaluation of a size measurement procedure for web applications," in *2008 Eighth International Conference on Web Engineering*. IEEE, 2008, pp. 217–223.

[248] S. Abrahão, G. Poels, and O. Pastor, "Comparative evaluation of functional size measurement methods: An experimental analysis," *Department of Computer Science and Computation, Valencia University of Technology, Belgium*, 2004.

[249] F. Paz, F. A. Paz, J. J. Arenas, and C. Rosas, "A perception study of a new set of usability heuristics for transactional web sites," *Intelligent Human Systems Integration: Proceedings of the 1st International Conference on Intelligent Human Systems Integration (IHSI 2018): Integrating People and Intelligent Systems, January 7-9, 2018, Dubai, United Arab Emirates*, pp. 620–625, 2018.

[250] J. Díaz, J. Arango-López, S. Sepúlveda, D. Ahumada, F. Moreira, and J. Gebauer, "A virtual reality approach to automatic blood sample generation," *Trends and Innovations in Information Systems and Technologies: Volume 2 8*, pp. 221–230, 2020.

[251] J. Díaz, J. A. Lopez, S. Sepúlveda, G. M. R. Villegas, D. Ahumada, and F. Moreira, "Evaluating aspects of usability in video game-based programming learning platforms," *Procedia Computer Science*, vol. 181, pp. 247–254, 2021.

[252] S. Abrahao and G. Poels, "Further analysis on the evaluation of a size measure for web applications," *2006 Fourth Latin American Web Congress*, pp. 230–240, 2006.

[253] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly: Management Information Systems*, vol. 13, pp. 319–339, 1989.

[254] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," *Management Science*, vol. 35, pp. 982–1003, 1989.

[255] Y. Cherdantseva, "Secure * BPMN - A graphical extension for BPMN 2.0 based on a reference model of information assurance & security," Ph.D. dissertation, Cardiff University, 2014.

[256] F. Gonzalez-Lopez and G. Bustos, "Evaluating methodologies for business process architecture design-a pilot study," in *ZEUS*, 2019, pp. 1–8. [Online]. Available: http://ceur-ws.org/Vol-2339

[257] G. Albaum, "The likert scale revisited," in *Market Research Society. Journal.*, vol. 39. SAGE Publications Sage UK: London, England, 1997, pp. 1–21.

[258] T. Nemoto and D. Beglar, "Likert-scale questionnaires," in *JALT 2013 conference proceedings*, 2014, pp. 1–8.

[259] A. P. King and R. J. Eckersley, "Inferential Statistics IV: Choosing a Hypothesis Test," in *Statistics for Biomedical Engineers and Scientists: How to visualize and analyze data*. Academic Press, 2019.

[260] H.-I. Park, "A generalization of wilcoxon rank sum test," *Applied Mathematical Sciences*, vol. 9, pp. 3155–3164, 2015. [Online]. Available: www.m-hikari.comhttp://dx.doi.org/10.12988/ams.2015.52129

Appendices

A Initial Template

1. The main functions of a SOC according to the existing SOC frameworks
    - 1.1 The Monitoring Function [21, 27, 52, 147]. This study examines the construct from SOC experts' perspective.
        - 1.1.1 Whose responsibility is it?
        - 1.1.2 Metrics for capturing performance under this function.
            - 1.1.2.1 Number of incidents detected [31, 39, 45, 52, 54, 56, 86]
            - 1.1.2.2 Mean Time To Detect an Incident [25, 52, 54, 72, 86]
    - 1.2 The Analysis Function [21, 27, 52, 147]. This work explores the construct from SOC experts' perspective.
        - 1.2.1 Whose responsibility is it?
        - 1.2.2 Metrics for capturing performance under this function.
            - 1.2.2.1 The quality of analysis [91]
            - 1.2.2.2 Number of alerts/events analysed [35, 45, 86, 87, 91]
    - 1.3 The Response Function [21, 27, 52, 56, 147]. This research explores the construct from SOC experts' perspective.
        - 1.3.1 Whose responsibility is it?
        - 1.3.2 Metrics for capturing performance under this function.
            - 1.3.2.1 Number of False Positives Reported [2, 52, 91]
            - 1.3.2.2 Number of True Positives Reported [2, 21, 52, 91]
            - 1.3.2.3 Number of Incidents Closed [56, 58, 86]
            - 1.3.2.4 Time of Ticket Creation [25, 54, 56, 86]
            - 1.3.2.5 Elapsed Time of Resolution [25, 56, 72]
            - 1.3.2.6 Time Taken to Mitigate [56, 72]
            - 1.3.2.7 Incident severity level [56, 72]
            - 1.3.2.8 Mean Time To Verify [72]
            - 1.3.2.9 Mean Time To Resolve [72]
            - 1.3.2.10 Mean Time To Fix [72]
    - 1.4 The Reporting Function [27, 52]. This study explores the construct from SOC experts' perspective.

1.4.1 Whose responsibility is it?

1.4.2 Metrics for capturing performance under this function.

1.4.2.1 The quality of an incident report [86, 199]

1.5 The Intelligence Function [21, 27]. This work seeks to understand the construct from SOC experts' perspective.

1.5.1 Whose responsibility is it?

1.5.2 Metrics for capturing performance under this function.

1.5.2.1 Number of Indicators of compromised detected over a rolling period [31]

1.6 The Vulnerability Function [21, 52]. This work seeks to understand the construct from SOC experts' perspective.

1.6.1 Whose responsibility is it?

1.6.2 Metrics for capturing performance under this function.

1.6.2.1 Number of vulnerabilities discovered [31, 56]

1.7 The Log Collection Function [52]. This work seeks to understand the construct from SOC experts' perspective.

1.7.1 Whose responsibility is it?

1.7.2 Metrics for capturing performance under this function.

1.7.2.1 No measure identified in existing literature

1.8 The Forensic Function [21]. This work seeks to understand the construct from SOC experts' perspective.

1.8.1 Whose responsibility is it?

1.8.2 Metrics for capturing performance under this function.

1.8.2.1 No measure identified in existing literature

1.9 The Penetration Testing Function [21]. This work seeks to examine the construct from SOC experts' perspective.

1.9.1 Whose responsibility is it?

1.9.2 Metrics for capturing performance under this function.

1.9.2.1 No measure identified in existing literature

1.10 The Baseline Security Function [21]. This work seeks to explore the construct from SOC experts' perspective.

1.10.1 Whose responsibility is it?

1.10.2 Metrics for capturing performance under this function.

1.10.2.1 No measure identified in existing literature

B Interview Questions

1. What is your job title and area of expertise? (Analyst, SOC Manager, SOC Engineer or SOC Consultant etc.)
2. How many years of SOC experience do you have, or have you had in the past?
3. Can you please tell us about your organisation?
4. Which of the functions of a SOC listed in the drafted template represents the activities of your SOC and the work of analysts?
5. Among the functions listed in the framework, which of them would you consider as the most important ones and why? Please explain.
6. In your opinion, are there other functional areas that you think should be included in the template? Please explain.

   The template suggests some measures for evaluating/assessing analysts' performance under each functional area. These measures are derived from literature and are listed under the heading subcriteria (measures).
7. In your current or previous work in the SOC, did you come across any metrics for measuring analysts' performance in the SOC? If you did, can you please elaborate on the nature of the metrics and how it was used?
8. What do you think are some of the advantages and disadvantages of the metrics you have come across? Please explain.
9. Ideally, how would you like an analyst's performance to be measured as he/she carries out tasks under the different functional areas identified in the framework? Please explain.
10. How often do you think analysts' performance should be measured? Daily/Weekly/Monthly?
11. Existing literature suggests that some SOCs measure analysts' performance based on the quality of the analysis. In your opinion, what would you consider as a good quality analysis?

12. Existing literature suggests that some SOCs measure analysts' performance based on the quality of their report. In your opinion, what would you consider as a good quality report?

13. Existing literature suggests that some SOCs use success stories to measure performance. In your opinion, what would you consider as a success story in a SOC? Can you give examples?

14. Finally, the template/framework is intended to represent the functions of a SOC, identify the functions of an analyst and performance metrics for analysts. In your opinion, is there anything that you would like to add in terms of the functions or areas of measure?

15. Is there anything else you would like to say?

Table 1: A template showing the SOC functions and performance metrics Identified in the literature.

SOC FUNCTIONS	A BRIEF DESCRIPTION OF THE FUNCTION	METRICS FOR MEASURING PERFORMANCE	Whose Responsibility is it?
Monitoring Function	• Real-Time Event Monitoring of an organisation's network traffic and enterprise information technology devices using solutions such as SIEM (Security, Incident and Event Management), IDS/IPS (Intrusion Detection Security/Intrusion Prevention Systems) to identify in a timely manner malicious or anomalies activities. • Monitor to detect policy violation, cyber-attacks, security breaches or any unusual activity on the network. • Monitoring of privilege user activities. • Identification of false positives and false negatives from sensors to decrease load on sensors and analysts. • Deep packet inspection and Alert Triage. • Use packet analysis tools such as TCPDump, Snort and Wireshark to detect malicious network activity.	Number of Incident Detected Time taken to Detect an Incident	
Analysis Function	• Analysing log files and event data reported by the monitoring and detection tools. • Visual inspection of logs and in-depth packet analysis of network traffic and alerts using a range of packet analyser tools such as Wireshark and TCPDump to establish whether an activity pose a threat to an organisation. • Draws on historical logs to confirm trends and patterns. • Conducting root cause analysis and creating script queries to investigate logs. • Triage and Escalation Analysis	The quality of incident analysis Number of alerts/events analysed	
Response Function	• Isolation of suspicious devices to reduce damage to the enterprise network • Use incident tracking system to create and track tickets. • Writing reports	Number of False Positives Reported Number of True Positives Reported Number of Incidents Closed Time of Ticket Creation Elapsed Time of Resolution Time of Taken to Mitigate Incident severity level Mean Time to Verify Mean Time to Resolve Mean Time to Fix	
Reporting Function	Writing technical report on the incidents for relevant stakeholders	The quality of incident report	
Intelligence Function	• Identify threat actors that may pose danger to an organisation • Exchanging threat information with various internal and external parties. • Correlate information on various threats that might affect an organisation. • Blacklisting known malicious IP addresses such as those linked to command and control activities. • Creating intelligence use cases scenarios to track new and emerging threats. • Create event correlation rules and rules for event filtering.	Number of Indicators of Compromise Implemented	
Vulnerability Function	• Vulnerability Scans • Applying Patches to fix vulnerabilities.	Number of vulnerabilities discovered	
Log Collection Function	Deploying sensors to collect security logs	No metric identified in the existing literature	
Forensic Function	• Activities involves the identification, preservation, recovery, analysis and presentation of digital evidence to establish digital crime.	No metric identified in the existing literature	
Pentration (Pentest) Function	Use a range of security tools to test an organisation security defenses by simulating attacks against the network. Test a large number of systems for a variety of vulnerabilities. •Identify and exploit vulnerabilities in system(s) to assess security Support organisations to identify vulnerabilities as well as workable countermeasures, and help the bsuiness owners to determine how best to improve their security.	No metric identified in the existing literature	
Baseline Function	• Hardening systems, closing unused port, disabling unused services. • System Hardening by closing all unused ports and removal of unnecessary services. • Ensuring that systems are patched to the correct level and that all systems running unsupported operating systems are identified	No metric identified in the existing literature	

C SOC Functions, Analysts Functions and Metrics

Below are extracts of the functions of a SOC, analysts' functions, and metrics that can be used to evaluate analyst performance as reported by the participants.

1. The main functions of a SOC and the responsibilities of an analyst
    - 1.1 The Monitoring and Detection Function - Identified by the study participants as one of the primary functions of a SOC.
        - 1.1.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.
        - 1.1.2 Metrics for capturing performance under the Monitoring and Detection Function
            - 1.1.2.1 Number of misconfiguration detected
            - 1.1.2.2 Time taken to detect an incident
            - 1.1.2.3 Number of critical priority alert identified as an incident
            - 1.1.2.4 Number of high priority alert identified as an incident
            - 1.1.2.5 Number of medium priority alert identified as an incident
            - 1.1.2.6 Number of low priority alert identified as an incident
            - 1.1.2.7 In-house use case incidents detected
            - 1.1.2.8 Number of zero day incidents Detected
    - 1.2 The Analysis Function - Identified by the study participants as one of the primary functions of a SOC.
        - 1.2.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.
        - 1.2.2 Metrics for capturing performance under the Analysis Function
            - 1.2.2.1 Quality of the Analysis
            - 1.2.2.2 Number of critical priority alerts analysed
            - 1.2.2.3 Number of high priority alerts analysed
            - 1.2.2.4 Number of medium priority alerts analysed
            - 1.2.2.5 Number of low priority alerts analysed
    - 1.3 The Response and Reporting Function - Identified by the study participants as one of the primary functions of a SOC.

- 1.3.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.
- 1.3.2 Metrics for capturing performance under the Response and Reporting Function
  - 1.3.2.1 Quality of incident report
  - 1.3.2.2 Number of false positives reported
  - 1.3.2.3 Mean time to respond and mean time to mitigate
  - 1.3.2.4 Number of true critical incidents closed
  - 1.3.2.5 Number of true high incidents closed
  - 1.3.2.6 Number of true medium incidents closed
  - 1.3.2.7 Number of true low incidents closed
  - 1.3.2.8 Number of in-house use cases closed
  - 1.3.2.9 Number of zero-day incidents closed
  - 1.3.2.10 Mean time to respond/mean time to mitigate
- 1.4 The Intelligence Function - Identified as a SOC function by study participants.
  - 1.4.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.
  - 1.4.2 Metrics for capturing performance under the Intelligence Function
    - 1.4.2.1 Number of use cases created
    - 1.4.2.2 Number of indicators of compromise implemented
    - 1.4.2.3 Number of indicators of compromise shared
- 1.5 The Baseline and Vulnerability Function - Identified as a SOC function by study participants.
  - 1.5.1 Whose responsibility is it? - Reported by participants as an analyst responsibility
  - 1.5.2 Metrics for capturing performance under the Baseline and Vulnerability Function
    - 1.5.2.1 Number of patches applied
    - 1.5.2.2 Number of patches rolled back
    - 1.5.2.3 Number of vulnerabilities discovered
    - 1.5.2.4 Mean Time To Fix Vulnerability

1.6 Policies and signature management Function - Identified as a SOC function by study participants.

1.6.1 Whose responsibility is it? - Reported by participants as an analyst responsibility

1.6.2 Metrics for capturing performance under the policies and signature management function

1.6.2.1 Number of use cases amended

1.6.2.2 Number of use cases excluded

1.6.2.3 Number of false positives signatures excluded

1.7 Compliance and risk management Function - Identified as a SOC function by study participants.

1.7.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.

1.7.2 Metrics for capturing performance under the compliance and risk management function

1.7.2.1 No measures or Metrics reported by the participants

1.8 Incident Management Function - Identified as a SOC function by study participants.

1.8.1 Whose responsibility is it? - Reported by participants as an analyst responsibility.

1.8.2 Metrics for capturing performance under the incident management function

1.8.2.1 No measures or Metrics reported by the participants

1.9 The Penetration Testing Function - Identified as a SOC function by study participants.

1.9.1 Whose responsibility is it? - Reported by participants as a responsibility of a fully qualified penetration tester. This is not an analyst responsibility.

1.9.2 Metrics for capturing performance under the Penetration Testing Function

1.9.2.1 No measures or Metrics reported by the participants

1.10 The Forensic Function - Identified as a SOC function by study participants.

1.10.1 Whose responsibility is it? - Reported by participants as a responsibility of a fully qualified forensic specialist. This is not an analyst responsibility.

1.10.2 Metrics for capturing performance under the Forensic Function

1.10.2.1 No measures or Metrics reported by the participants

1.11 The Engineering and Log Collection Function - Identified as a SOC function by study participants.

1.11.1 Whose responsibility is it? - Reported by participants as a responsibility of a SOC Engineer. This is not an analyst responsibility.

1.11.2 Metric for capturing performance under the Engineering and Log Collection Function

1.11.2.1 No measures or Metrics reported by the participants

2. How should the performance of analysts be measured?

2.1 The quality of an analyst analysis and the quality of their incident report should be used as the measure of performance.

2.2 A quality analysis will investigate and report on the who, where, when, what, why, how and make a sound recommendation for addressing the report. These indicators are extracted and presented below:

2.2.1 **Who** Who caused the event? - the potential attackers or adversaries.

2.2.1.1 Attack Path (External threat or Insiders ?)

2.2.1.2 Source IP Address/Attacker IP Address

2.2.1.3 Source Port/Service

2.2.1.4 Source MAC Address

2.2.1.5 Attacker User Name (if internal)

2.2.1.6 Attacker Host Name

2.2.1.7 Attacker User Agent (if applicable)

2.2.2 **Where** - the direction or location of attack

2.2.2.1 Impacted host/application

2.2.2.2 Destination IP Address/Attacker IP Address

2.2.2.3 Destination Port/Service

2.2.2.4 Destination MAC Address

2.2.2.5 Location of Detection

2.2.3 **When** - the date and time when the attack was first detected

2.2.3.1 Date and time of detection including time zone

2.2.3.2 When did the event occur and the reporting Device

2.2.3.3 Detection time

2.2.3.4 Manager receipt time

2.2.4 **What** - the capabilities the attacker has or what they already know. What is the nature of the event?

2.2.4.1 Name of Alert/Incident/Trigger

2.2.4.2 File/Email/URL Domain Name

2.2.4.3 Asset Name

2.2.4.4 User Account

2.2.4.5 IPS Signature/Use Case

2.2.4.6 Event ID/Type/OS

2.2.4.7 Breach Type

2.2.4.8 Incident Severity/Classification

2.2.4.9 File Hash

2.2.4.10 Indicator of Compromise

2.2.5 **Why** - identified risk and reason for reporting the incident

2.2.5.1 Risk associated with the incident

2.2.5.2 Context of the incident including geographical Information and threat description

2.2.6 **How** - describes the method of detection

2.2.6.1 Method of Detection

2.2.6.2 Mitigation Factors

2.2.6.3 Playbook used (Enter playbook used for incident, if any(Phishing Playbook, Enrichment Playbook etc)

2.2.7 **Recommendations** - steps taken to address the identified incident.

2.2.7.1 Recommended containment strategy

2.2.7.2 Recommended mitigation strategy

2.2.7.3 Any contact details (E.g. Email, Phone number, Office) - for further investigation

2.2.7.4 Creation of a new use case or signature (if required)

Table 2: A template showing SOC functions, Analysts Functions and Performance Metrics.

SOC FUNCTIONS	A BRIEF DESCRIPTION OF THE FUNCTION	METRICS FOR MEASURING PERFORMANCE	Whose Responsibility is it?
Monitoring and Detection Function	• Real-Time Event Monitoring of an organisation's network traffic and enterprise information technology devices using solutions such as SIEM (Security, Incident and Event Management), IDS/IPS (Intrusion Detection Security/Intrusion Prevention Systems) to identify in a timely manner malicious or anomalies activities. • Monitor to detect policy violation, cyber-attacks, security breaches or any unusual activity on the network. • Monitoring of privilege user activities. • Identification of false positives and false negatives from sensors to decrease load on sensors and analysts. • Deep packet inspection and Alert Triage. • Use packet analysis tools such as TCPDump, Snort and Wireshark to detect malicious network activity.	Number of misconfigurations detected Time taken to detect an incident Number of critical priority alerts identified as an incident Number of high priority alerts identified as an incident Number of medium priority alerts identified as an incident Number of low priority alerts identified as an incident In-house use case incidents detected Number of zero-day incidents Detected	A SOC Analyst
Analysis Function	• Analysing log files and event data reported by the monitoring and detection tools. • Visual inspection of logs and in-depth packet analysis of network traffic and alerts using a range of packet analyser tools such as Wireshark and TCPDump to establish whether an activity pose a threat to an organisation. • Draws on historical logs to confirm trends and patterns. • Conducting root cause analysis and creating script queries to investigate logs. • Triage and Escalation Analysis	Quality of the Analysis Number of critical priority alerts analysed Number of high priority alerts analysed Number of medium priority alerts analysed Number of low priority alerts analysed	A SOC Analyst
Response and Reporting Function	• Isolation of suspicious devices to reduce damage to the enterprise network • Use incident tracking system to create and track tickets. • Writing reports	Quality of incident report Number of false positives Reported Mean time to respond and mean time to mitigate Number of true critical incidents closed Number of true high incidents closed Number of true medium incidents closed Number of true low incidents closed Number of in-house use cases closed Number of zero-day incidents closed Mean time to respond/mean time to mitigate	A SOC Analyst
Intelligence Function	• Identify threat actors that may pose danger to an organisation • Exchanging threat information with various internal and external parties. • Correlate information on various threats that might affect an organisation. • Blacklisting known malicious IP addresses such as those linked to command and control activities. • Creating intelligence use cases scenarios to track new and emerging threats. • Create event correlation rules and rules for event filtering.	Number of use cases created Number of indicators of compromise implemented Number of indicators of compromise shared	A SOC Analyst
Baseline and Vulnerability Function	• Vulnerability Scans • Applying Patches to fix vulnerabilities. • Hardening systems, closing unused port, disabling unused services. • System Hardening by closing all unused ports and removal of unnecessary services. • Ensuring that systems are patched to the correct level and that all systems running unsupported operating systems are identified	Number of patches applied Number of patches rolled back Number of vulnerabilities discovered Mean Time To Fix Vulnerability	A SOC Analyst
Policies and Signature Management	• Writing and Tuning Correlation Rules • Content Modification to remove false positives. • Content Modification to remove false positives.	Number of use cases amended Number of use cases excluded Number of false positives signatures excluded	A SOC Analyst
Compliance and Risk Management Function	• Compliance Scans • Reporting on system security state as dictated by industry and/or regulatory requirment.	No specific metrics are suggested.	A SOC Analyst
Incident Management/Handling Function	• Partly covered by an analyst, but predomintely carried out by Incident Handlers working in a Computer Security Incident and Reponse Team (CSIRT)	No specific metrics are suggested.	A SOC Analyst
Pentration (Pentest) Function/Red Team	Use a range of security tools to test an organisation security defenses by simulating attacks against the network. Test a large number of systems for a variety of vulnerabilities. •Identify and exploit vulnerabilities in system(s) to assess security Support organisations to identify vulnerabilities as well as workable countermeasures, and help the bsuiness owners to determine how best to improve their security.	No specific metrics are suggested.	A Pentester
Forensic and Malware Analysis Function	• Activities involves the identification, preservation, recovery, analysis and presentation of digital evidence to establish digital crime.	No specific metrics are suggested.	A Forensic Specialist
Engineering and Collection Function	Deploying sensors to collect security logs	No specific metrics are suggested.	A SOC Engineer

D Participants' Responses for the Main Criteria

Table 3: Participant 1: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	3	3	1	3
Analysis Function	1	1	3	3	1	3
Baseline and Vulnerability Function	1/3	1/3	1	1/3	1/3	1
Intelligence Function	1/3	1/3	3	1	1/3	3
Response and Reporting Function	1	1	3	3	1	3
Policies and Signature Function	1/3	1/3	1	1/3	1/3	1

Table 4: Participant 2: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	5	5	1	1
Analysis Function	1	1	5	3	1	1
Baseline and Vulnerability Function	1/5	1/5	1	1	1	1/3
Intelligence Function	1/5	1/3	1	1	1	1
Response and Reporting Function	1	1	1	1	1	1/3
Policies and Signature Function	1	1	3	1	3	1

Table 5: Participant 3: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	1	1	1	1
Analysis Function	1	1	1	1	1	1
Baseline and Vulnerability Function	1	1	1	1	1	1
Intelligence Function	1	1	1	1	1	1
Response and Reporting Function	1	1	1	1	1	1
Policies and Signature Function	1	1	1	1	1	1

Table 6: Participant 4: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	3	3	1	3
Analysis Function	1	1	3	3	1	3
Baseline and Vulnerability Function	1/3	1/3	1	1/3	1/3	1
Intelligence Function	1/3	1/3	3	1	1/3	3
Response and Reporting Function	1	1	3	3	1	3
Policies and Signature Function	1/3	1/3	1	1/3	1/3	1

Table 7: Participant 5: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	4	3	1	2
Analysis Function	1	1	3	2	1	3
Baseline and Vulnerability Function	1/4	1/3	1	1	1	1
Intelligence Function	1/3	1/2	1	1	1	2
Response and Reporting Function	1	1	1	1	1	3
Policies and Signature Function	1/2	1/3	1	1/2	1/3	1

Table 8: Participant 6: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	3	3	3	4	7
Analysis Function	1/3	1	1	1	4	5
Baseline and Vulnerability Function	1/3	1	1	1	3	5
Intelligence Function	1/3	1	1	1	3	5
Response and Reporting Function	1/4	1/4	1/3	1/3	1	3
Policies and Signature Function	1/7	1/5	1/5	1/5	1/3	1

Table 9: Participant 7: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1/3	3	3	3	3
Analysis Function	3	1	7	7	1	7
Baseline and Vulnerability Function	1/3	1/7	1	1	1	3
Intelligence Function	1/3	1/7	1	1	1	3
Response and Reporting Function	1/3	1	1	1	1	3
Policies and Signature Function	1/3	1/7	1/3	1/3	1/3	1

Table 10: Participant 8: Comparison Matrix for the Main Criteria

Criteria	Monitoring and Detection Function	Analysis Function	Baseline and Vulnerability Function	Intelligence Function	Response and Reporting Function	Policies and Signature Function
Monitoring and Detection Function	1	1	3	3	1	2
Analysis Function	1	1	3	2	1	2
Baseline and Vulnerability Function	1/3	1/3	1	1	1/2	3
Intelligence Function	1/3	1/2	1	1	1/2	2
Response and Reporting Function	1	1	2	2	1	2
Policies and Signature Function	1/2	1/2	1/3	1/2	1/2	1

E Participants' Responses for the Monitoring and Detection Function

Table 11: Participant 1: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/3	1	1	3	1	1/3
Number of Critical Incidents Detected over a rolling period	3	1	1	1	3	1	1/2
Number of High Incidents Detected over a rolling period	1	1	1	1	3	1	1/2
Number of Medium Incidents Detected over a rolling period	1	1	1	1	3	1	1/3
Number of Low Incidents Detected over a rolling period	1/3	1/3	1/3	1/3	1	1/3	1/3
Number of Use Case Incidents Detected over a rolling period	1	1	1	1	3	1	1/3
Number of Zero Day Incidents Detected over a rolling period	3	2	2	3	3	3	1

Table 12: Participant 2: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/9	1/9	1/9	1/9	1/9	1/9
Number of Critical Incidents Detected over a rolling period	9	1	1	1	3	1	1/2
Number of High Incidents Detected over a rolling period	9	1	1	3	3	1	1/2
Number of Medium Incidents Detected over a rolling period	9	1	1/3	1	3	1	1/9
Number of Low Incidents Detected over a rolling period	9	1/3	1/3	1/3	1	1/2	1/9
Number of Use Case Incidents Detected over a rolling period	9	1	1	1	2	1	1/9
Number of Zero Day Incidents Detected over a rolling period	9	2	2	9	9	9	1

Table 13: Participant 3: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/3	1/3	1/2	3	1/3	1/3
Number of Critical Incidents Detected over a rolling period	3	1	3	5	7	1/3	1/3
Number of High Incidents Detected over a rolling period	3	1/3	1	3	5	1/3	1/3
Number of Medium Incidents Detected over a rolling period	2	1/5	1/3	1	3	1/5	1/4
Number of Low Incidents Detected over a rolling period	1/3	1/7	1/5	1/3	1	1/7	1/4
Number of Use Case Incidents Detected over a rolling period	3	3	3	5	7	1	1/2
Number of Zero Day Incidents Detected over a rolling period	3	3	3	4	4	2	1

Table 14: Participant 4: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/5	1/3	1/2	3	1	1/4
Number of Critical Incidents Detected over a rolling period	5	1	1	1	3	1	1/2
Number of High Incidents Detected over a rolling period	3	1	1	1	3	1	1/2
Number of Medium Incidents Detected over a rolling period	2	1	1	1	3	1	1/3
Number of Low Incidents Detected over a rolling period	1/3	1/3	1/3	1/3	1	1/3	1/3
Number of Use Case Incidents Detected over a rolling period	1	1	1	1	3	1	1/3
Number of Zero Day Incidents Detected over a rolling period	4	2	2	3	3	3	1

Table 15: Participant 5: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/5	1/3	1	2	1	1/4
Number of Critical Incidents Detected over a rolling period	5	1	1	1	4	1	1
Number of High Incidents Detected over a rolling period	3	1	1	2	3	1	1/4
Number of Medium Incidents Detected over a rolling period	1	1	1/2	1	2	1/2	1/2
Number of Low Incidents Detected over a rolling period	1/2	1/4	1/3	1/2	1	1/5	1/5
Number of Use Case Incidents Detected over a rolling period	1	1	1	2	5	1	1/3
Number of Zero Day Incidents Detected over a rolling period	4	1	4	2	5	3	1

Table 16: Participant 6: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/9	1/7	1/3	1	1	1/9
Number of Critical Incidents Detected over a rolling period	9	1	5	7	9	7	1
Number of High Incidents Detected over a rolling period	7	1/5	1	5	7	5	1/5
Number of Medium Incidents Detected over a rolling period	3	1/7	1/5	1	5	3	1/7
Number of Low Incidents Detected over a rolling period	1	1/9	1/7	1/5	1	1	1/9
Number of Use Case Incidents Detected over a rolling period	1	1/7	1/5	1/3	1	1	1/9
Number of Zero Day Incidents Detected over a rolling period	9	1	5	7	9	9	1

Table 17: Participant 7: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1	1	1	3	1/3	1/3
Number of Critical Incidents Detected over a rolling period	1	1	3	3	7	1/3	1/5
Number of High Incidents Detected over a rolling period	1	1/3	1	3	5	1/3	1/3
Number of Medium Incidents Detected over a rolling period	1	1/3	1/3	1	3	1/3	1/3
Number of Low Incidents Detected over a rolling period	1/3	1/7	1/5	1/3	1	1/3	1/7
Number of Use Case Incidents Detected over a rolling period	3	3	3	3	3	1	1
Number of Zero Day Incidents Detected over a rolling period	3	5	3	3	7	1	1

Table 18: Participant 8: Comparison Matrix for the Monitoring and Detection Function.

Subcriteria	Number of Misconfiguration Detected over a rolling period	Number of Critical Incidents Detected over a rolling period	Number of High Incidents Detected over a rolling period	Number of Medium Incidents Detected over a rolling period	Number of Low Incidents Detected over a rolling period	Number of Use Case Incidents Detected over a rolling period	Number of Zero Day Incidents Detected over a rolling period
Number of Misconfiguration Detected over a rolling period	1	1/5	1/3	1/2	1	1/2	1/5
Number of Critical Incidents Detected over a rolling period	5	1	1	1	4	1	1
Number of High Incidents Detected over a rolling period	3	1	1	2	3	1	1/7
Number of Medium Incidents Detected over a rolling period	2	1	1/2	1	3	1	1/6
Number of Low Incidents Detected over a rolling period	1	1/4	1/3	1/3	1	1/6	1/5
Number of Use Case Incidents Detected over a rolling period	2	1	1	1	6	1	1/2
Number of Zero Day Incidents Detected over a rolling period	5	1	7	6	5	2	1

F Participants' Responses for the Analysis Function

Table 19: Participant 1: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	5	5	5	5	5	5
Number of Critical Priority Alert Analysed over a rolling period	1/5	1	1	1	3	1	1/2
Number of High Priority Alert Analysed over a rolling period	1/5	1	1	1	3	1	1/2
Number of Medium Priority Alert Analysed over a rolling period	1/5	1	1	1	3	1	1/3
Number of Low Priority Alert Analysed over a rolling period	1/5	1/3	1/3	1/3	1	1/3	1/3
Number of In-house Use case Analysed over a rolling period	1/5	1	1	1	3	1	1/3
Number of Zero Day Incidents Analysed over a day rolling period	1/5	2	2	3	3	3	1

Table 20: Participant 2: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	5	5	5	5	5	5
Number of Critical Priority Alert Analysed over a rolling period	1/5	1	1	1	5	1	1/3
Number of High Priority Alert Analysed over a rolling period	1/5	1	1	3	3	1	1/3
Number of Medium Priority Alert Analysed over a rolling period	1/5	1	1/3	1	3	1	1/9
Number of Low Priority Alert Analysed over a rolling period	1/5	1/5	1/3	1/3	1	1/3	1/9
Number of In-house Use case Analysed over a rolling period	1/5	1	1	1	3	1	1/9
Number of Zero Day Incidents Analysed over a day rolling period	1/5	3	3	9	9	9	1

Table 21: Participant 3: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	3	5	7	7	3	3
Number of Critical Priority Alert Analysed over a rolling period	1/3	1	3	5	7	1/2	1/5
Number of High Priority Alert Analysed over a rolling period	1/5	1/3	1	3	5	1/5	1/5
Number of Medium Priority Alert Analysed over a rolling period	1/7	1/5	1/3	1	3	1/5	1/8
Number of Low Priority Alert Analysed over a rolling period	1/7	1/7	1/5	1/3	1	1/5	1/8
Number of In-house Use case Analysed over a rolling period	1/3	2	5	5	5	1	1/3
Number of Zero Day Incidents Analysed over a day rolling period	1/3	5	5	8	8	3	1

Table 22: Participant 4: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	5	5	5	5	5	5
Number of Critical Priority Alert Analysed over a rolling period	1/5	1	2	3	3	3	1/2
Number of High Priority Alert Analysed over a rolling period	1/5	1/2	1	1	2	1	1/2
Number of Medium Priority Alert Analysed over a rolling period	1/5	1/3	1	1	1	1	1/3
Number of Low Priority Alert Analysed over a rolling period	1/5	1/3	1/2	1	1	1/3	1/3
Number of In-house Use case Analysed over a rolling period	1/5	1/3	1	1	3	1	1/3
Number of Zero Day Incidents Analysed over a day rolling period	1/5	2	2	3	3	3	1

Table 23: Participant 5: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	4	5	5	5	4	4
Number of Critical Priority Alert Analysed over a rolling period	1/4	1	2	2	4	1	2
Number of High Priority Alert Analysed over a rolling period	1/5	1/2	1	2	2	1	1/4
Number of Medium Priority Alert Analysed over a rolling period	1/5	1/2	1/2	1	2	1	1/4
Number of Low Priority Alert Analysed over a rolling period	1/5	1/4	1/2	1/2	1	1/5	1/3
Number of In-house Use case Analysed over a rolling period	1/4	1	1	1	5	1	1
Number of Zero Day Incidents Analysed over a day rolling period	1/4	1/2	4	4	3	1	1

Table 24: Participant 6: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	9	9	9	9	9	1
Number of Critical Priority Alert Analysed over a rolling period	1/9	1	1	1	1	1	1
Number of High Priority Alert Analysed over a rolling period	1/9	1	1	1	1	1	1
Number of Medium Priority Alert Analysed over a rolling period	1/9	1	1	1	1	1	1
Number of Low Priority Alert Analysed over a rolling period	1/9	1	1	1	1	1	1
Number of In-house Use case Analysed over a rolling period	1/9	1	1	1	1	1	1
Number of Zero Day Incidents Analysed over a day rolling period	1	1	1	1	1	1	1

Table 25: Participant 7: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	5	5	5	5	5	5
Number of Critical Priority Alert Analysed over a rolling period	1/5	1	1	3	3	1	1/3
Number of High Priority Alert Analysed over a rolling period	1/5	1	1	1	5	3	1/2
Number of Medium Priority Alert Analysed over a rolling period	1/5	1/3	1	1	3	1	1/3
Number of Low Priority Alert Analysed over a rolling period	1/5	1/3	1/5	1/3	1	1/3	1/2
Number of In-house Use case Analysed over a rolling period	1/5	1	1/3	1	3	1	1
Number of Zero Day Incidents Analysed over a day rolling period	1/5	3	2	3	2	1	1

Table 26: Participant 8: Comparison Matrix for the Analysis Function

Subcriteria	Quality of Analysis	Number of Critical Priority Alert Analysed over a rolling period	Number of High Priority Alert Analysed over a rolling period	Number of Medium Priority Alert Analysed over a rolling period	Number of Low Priority Alert Analysed over a rolling period	Number of In-house Use case Analysed over a rolling period	Number of Zero Day Incidents Analysed over a day rolling period
Quality of Analysis	1	7	7	7	7	7	4
Number of Critical Priority Alert Analysed over a rolling period	1/7	1	2	2	4	1	1
Number of High Priority Alert Analysed over a rolling period	1/7	1/2	1	2	3	1	1
Number of Medium Priority Alert Analysed over a rolling period	1/7	1/2	1/2	1	2	1	1/9
Number of Low Priority Alert Analysed over a rolling period	1/7	1/4	1/3	1/2	1	1/5	1/5
Number of In-house Use case Analysed over a rolling period	1/7	1	1	1	5	1	1
Number of Zero Day Incidents Analysed over a day rolling period	1/4	1	1	9	5	1	1

G Participants' Responses for the Response and Reporting Function

Table 27: Participant 1: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	5	5	5	5	5	5	5
Number of False Positives Reported over a rolling period	1/5	1	1/3	1/3	1	1	1	1/3
Number of True Critical Incident Closed over a rolling period	1/5	3	1	1	1	1	1	1/2
Number of True High Incident Closed over a rolling period	1/5	3	1	1	1	1	1	1/2
Number of True Medium Incident Closed over a rolling period	1/5	1	1	1	1	1	1	1/3
Number of True Low Incident Closed over a rolling period	1/5	1	1	1	1	1	1	1/3
Number of In-house Use Case Incidents Closed over a rolling period	1/5	1	1	1	1	1	1	1/2
Number of Zero Day Closed over a rolling period	1/5	3	2	2	3	3	2	1

Table 28: Participant 2: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	5	5	5	5	5	5	5
Number of False Positives Reported over a rolling period	1/5	1	1/9	1/9	1/9	1/9	1/9	1/9
Number of True Critical Incident Closed over a rolling period	1/5	9	1	1	1	1	1	1
Number of True High Incident Closed over a rolling period	1/5	9	1	1	3	3	3	1
Number of True Medium Incident Closed over a rolling period	1/5	9	1	1/3	1	1	1	1
Number of True Low Incident Closed over a rolling period	1/5	9	1	1/3	1	1	1	1/3
Number of In-house Use Case Incidents Closed over a rolling period	1/5	9	1	1/3	1	1	1	1/3
Number of Zero Day Closed over a rolling period	1/5	9	1	1	1	3	3	1

Table 29: Participant 3: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	7	5	6	7	7	3	3
Number of False Positives Reported over a rolling period	1/7	1	1/5	1/3	1	1	1/5	1/5
Number of True Critical Incident Closed over a rolling period	1/5	5	1	3	5	7	1/3	1/3
Number of True High Incident Closed over a rolling period	1/6	3	1/3	1	3	5	1/5	1/5
Number of True Medium Incident Closed over a rolling period	1/7	1	1/5	1/3	1	3	1/7	1/7
Number of True Low Incident Closed over a rolling period	1/7	1	1/7	1/5	1/3	1	1/7	1/7
Number of In-house Use Case Incidents Closed over a rolling period	1/3	5	3	5	7	7	1	1/3
Number of Zero Day Closed over a rolling period	1/3	5	3	5	7	7	3	1

Table 30: Participant 4: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	5	5	5	5	5	5	5
Number of False Positives Reported over a rolling period	1/5	1	1/3	1/3	1/3	1/2	1	1/3
Number of True Critical Incident Closed over a rolling period	1/5	3	1	1	1	1	1	1/2
Number of True High Incident Closed over a rolling period	1/5	3	1	1	1	1	1	1/2
Number of True Medium Incident Closed over a rolling period	1/5	3	1	1	1	1	1	1/3
Number of True Low Incident Closed over a rolling period	1/5	2	1	1	1	1	1	1/3
Number of In-house Use Case Incidents Closed over a rolling period	1/5	1	1	1	1	1	1	1/2
Number of Zero Day Closed over a rolling period	1/5	3	2	2	3	3	2	1

Table 31: Participant 5: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	3	5	5	5	5	4	4
Number of False Positives Reported over a rolling period	1/3	1	1/3	1/3	1	1	1/5	1/5
Number of True Critical Incident Closed over a rolling period	1/5	3	1	2	1	2	1	1
Number of True High Incident Closed over a rolling period	1/5	3	1/2	1	2	2	1	1
Number of True Medium Incident Closed over a rolling period	1/5	1	1	1/2	1	2	2	1/4
Number of True Low Incident Closed over a rolling period	1/5	1	1/2	1/2	1/2	1	1/3	1/5
Number of In-house Use Case Incidents Closed over a rolling period	1/4	5	1	1	1/2	3	1	1/6
Number of Zero Day Closed over a rolling period	1/4	5	1	1	4	5	6	1

Table 32: Participant 6: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	9	9	9	9	9	9	3
Number of False Positives Reported over a rolling period	1/9	1	1/3	1/3	1	1	1	1/3
Number of True Critical Incident Closed over a rolling period	1/9	3	1	1	1	1	3	1
Number of True High Incident Closed over a rolling period	1/9	3	1	1	3	3	3	1/5
Number of True Medium Incident Closed over a rolling period	1/9	1	1	1/3	1	2	1	1/7
Number of True Low Incident Closed over a rolling period	1/9	1	1	1/3	1/2	1	1	1/7
Number of In-house Use Case Incidents Closed over a rolling period	1/9	1	1/3	1/3	1	1	1	1/7
Number of Zero Day Closed over a rolling period	1/3	3	1	5	7	7	7	1

Table 33: Participant 7: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	5	3	3	5	5	1	1
Number of False Positives Reported over a rolling period	1/5	1	1/3	1/3	1	1	1	1/9
Number of True Critical Incident Closed over a rolling period	1/3	3	1	1	3	3	1	1/3
Number of True High Incident Closed over a rolling period	1/3	3	1	1	3	5	1	1/3
Number of True Medium Incident Closed over a rolling period	1/5	1	1/3	1/3	1	3	1	1/3
Number of True Low Incident Closed over a rolling period	1/5	1	1/3	1/5	1/3	1	1	1/3
Number of In-house Use Case Incidents Closed over a rolling period	1	1	1	1	1	1	1	1/3
Number of Zero Day Closed over a rolling period	1	9	3	3	3	3	3	1

Table 34: Participant 8: Comparison Matrix for the Response and Reporting Function.

Subcriteria	Quality of Incident Report	Number of False Positives Reported over a rolling period	Number of True Critical Incident Closed over a rolling period	Number of True High Incident Closed over a rolling period	Number of True Medium Incident Closed over a rolling period	Number of True Low Incident Closed over a rolling period	Number of In-house Use Case Incidents Closed over a rolling period	Number of Zero Day Closed over a rolling period
Quality of Incident Report	1	5	3	3	3	3	3	3
Number of False Positives Reported over a rolling period	1/5	1	1	1	1/2	1	1	1/3
Number of True Critical Incident Closed over a rolling period	1/3	1	1	2	3	3	1	1
Number of True High Incident Closed over a rolling period	1/3	1	1/2	1	2	3	1/2	1
Number of True Medium Incident Closed over a rolling period	1/3	2	1/3	1/2	1	3	1/3	1/3
Number of True Low Incident Closed over a rolling period	1/3	1	1/3	1/3	1/3	1	1	1/8
Number of In-house Use Case Incidents Closed over a rolling period	1/3	1	1	2	3	1	1	1/3
Number of Zero Day Closed over a rolling period	1/3	3	1	1	3	8	3	1

H Participants' Responses for the Intelligence Function

Table 35: Participant 1: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1	2
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	1
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/2	1	1

Table 36: Participant 2: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1	5
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	7
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/5	1/7	1

Table 37: Participant 3: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	3	3
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1/3	1	1
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/3	1	1

Table 38: Participant 4: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1/3	1/2
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	3	1	1
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2	1	1

Table 39: Participant 5: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1	2
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	1
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/2	1	1

Table 40: Participant 6: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1/7	1/5
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	7	1	3
Number of Indicators of Compromised (IOCs) Shared over a rolling period	5	1/3	1

Table 41: Participant 7: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1	7
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	7
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/7	1/7	1

Table 42: Participant 8: Comparison Matrix for the Intelligence Function

Subcriteria	Number of Use Cases Created over a rolling period	Number of Indicators of Compromised (IOCs) Implemented over a rolling period	Number of Indicators of Compromised (IOCs) Shared over a rolling period
Number of Use Cases Created over a rolling period	1	1	5
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	1	1	3
Number of Indicators of Compromised (IOCs) Shared over a rolling period	1/5	1/3	1

I Participants' Responses for the Baseline and Vulnerability Function

Table 43: Participant 1: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	3	1/3
Number of Patches Rolled back over a rolling period	1/3	1	1/4
Number of Vulnerabilities Discovered over a rolling period	3	4	1

Table 44: Participant 2: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	9	1
Number of Patches Rolled back over a rolling period	1/9	1	1/9
Number of Vulnerabilities Discovered over a rolling period	1	9	1

Table 45: Participant 3: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	1	1
Number of Patches Rolled back over a rolling period	1	1	1
Number of Vulnerabilities Discovered over a rolling period	1	1	1

Table 46: Participant 4: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	1	1/3
Number of Patches Rolled back over a rolling period	1	1	1/4
Number of Vulnerabilities Discovered over a rolling period	3	4	1

Table 47: Participant 5: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	1	1/3
Number of Patches Rolled back over a rolling period	1	1	1/2
Number of Vulnerabilities Discovered over a rolling period	3	2	1

Table 48: Participant 6: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	5	1/3
Number of Patches Rolled back over a rolling period	1/5	1	1/7
Number of Vulnerabilities Discovered over a rolling period	3	7	1

Table 49: Participant 7: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	1	3
Number of Patches Rolled back over a rolling period	1	1	2
Number of Vulnerabilities Discovered over a rolling period	1/3	1/2	1

Table 50: Participant 8: Comparison Matrix for the Baseline and Vulnerability Function.

Subcriteria	Number of Patches Applied over a rolling period	Number of Patches Rolled back over a rolling period	Number of Vulnerabilities Discovered over a rolling period
Number of Patches Applied over a rolling period	1	2	1
Number of Patches Rolled back over a rolling period	1/2	1	1/5
Number of Vulnerabilities Discovered over a rolling period	1	5	1

J Participants' Responses for the Policies and Signature Mgmt. Function

Table 51: Participant 1: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1/3	1
Number of Use Cases or Signatures Amended over a rolling period	3	1	3
Number of False Positives Signatures Excluded over a rolling period	1	1/3	1

Table 52: Participant 2: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1	1/9
Number of Use Cases or Signatures Amended over a rolling period	1	1	1/9
Number of False Positives Signatures Excluded over a rolling period	9	9	1

Table 53: Participant 3: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1	1
Number of Use Cases or Signatures Amended over a rolling period	1	1	1
Number of False Positives Signatures Excluded over a rolling period	1	1	1

Table 54: Participant 4: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1	1
Number of Use Cases or Signatures Amended over a rolling period	1	1	1
Number of False Positives Signatures Excluded over a rolling period	1	1	1

Table 55: Participant 5: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1/3	1
Number of Use Cases or Signatures Amended over a rolling period	3	1	3
Number of False Positives Signatures Excluded over a rolling period	1	1/3	1

Table 56: Participant 6: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1	1
Number of Use Cases or Signatures Amended over a rolling period	1	1	1
Number of False Positives Signatures Excluded over a rolling period	1	1	1

Table 57: Participant 7: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1/3	1
Number of Use Cases or Signatures Amended over a rolling period	3	1	3
Number of False Positives Signatures Excluded over a rolling period	1	1/3	1

Table 58: Participant 8: Comparison Matrix for the Policies and Signature Mgmt. Function.

Subcriteria	Number of Use Cases Excluded over a rolling period	Number of Use Cases or Signatures Amended over a rolling period	Number of False Positives Signatures Excluded over a rolling period
Number of Use Cases Excluded over a rolling period	1	1/7	1
Number of Use Cases or Signatures Amended over a rolling period	7	1	5
Number of False Positives Signatures Excluded over a rolling period	1	1/5	1

K Post-Testing Survey Questionnaire

1. What is your role title in your organisation?

   [] SOC Manager

   [] SOC Analyst

   [] Other

2. Which industry do you work in?

   [] Information Technology

   [] Airline and Aerospace

   [] Defence

   [] Banking and Finance

   [] Construction and Transportation

   [] Managed Security Service Provider (MSSP)

   [] Health and Social Care

   [] Telecommunication

   [] Other

3. How many years of SOC experience do you have?

   _____-

   For each of the questions below, select the response that best characterises how you feel about the statement, where: 1= Strongly Disagree, 2= Disagree, 3= Neither Agree Nor Disagree, 4 = Agree, and 5= Strongly Agree.

   Perceived Usefulness (PU) of the SOC-AAM

4. Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.

   [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

5. I find the SOC-AAM useful for achieving the purpose of measuring an analyst's performance.

[] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

6. The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.

   [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

   Perceived Ease of Use of the SOC-AAM

7. I found the procedure for applying the SOC-AAM easy to follow.

   [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

8. Overall, I found the SOC-AAM easy to use.

   [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

9. I found the SOC-AAM easy to learn.

   [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

10. The SOC-AAM is clear and easy to grasp.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

    Intention to Use the SOC-AAM

11. If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

12. In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

13. I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

    Perceived Completeness (PCO) of the SOC-AAM

14. I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

15. I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.

    [] Strongly disagree [] Disagree [] Neither agree nor disagree [] Agree [] Strongly agree

    Analysts Only

16. In your opinion, did the introduction of the SOC-AAM lead to an improvement in yur performance, or did it not make any difference to their performance?

    _____

    Managers Only

17. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance?

    _____

18. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team?

    _____

L Participants' Responses to the Survey Items

Participant P1

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- (●) SOC Manager
- ( ) SOC Analyst
- ( ) Other: .....

2. Which industry do you work in? *

- ( ) Information Technology
- ( ) Airline and Aerospace
- ( ) Defence
- ( ) Banking and Finance
- ( ) Construction and Transportation
- ( ) Managed Security Service Provider (MSSP)
- ( ) Health and Social Care
- (●) Telecommunication
- ( ) Other: .....

3. How many years of SOC experience do you have? *

5 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

In my opinion I think the SOC-AAM greatly help my analysts develop their ability to analyze events. I think the quality of analysis criteria is good but it comes with experience, knowledge and also process of the organisation.

In the SOC-AAM, all the important functions of the analysis are assessed, and the assessment is described in detail in accordance with the team's work.

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

In my opinion the SOC-AAM reflect more than 95% of the team's performance in incident analysis. I think it can be improved by allowing the manager to also assign about 5% score to analysts on their overall productivity.

But at the same time, the teams at dtac also have different individual functions for example implementation and architect role which is not in the SOC-AAM. Therefore, when the results are collected for each period, there will be times when the outcome will not be linear because the analyst were performing other implementation activities. But overall, when compared to the general SOC, I think the SOC-AAM is satisfactory in measuring analyst performance.

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

Participant P2

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ○ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ◉ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

3 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I am very happy using this method because it concentrate on the area of my work that can be measured. I will say it is tangible. I am also happy that the weights for the different tasks are not the same because when I work on high priority incident I don't want to have the same score as someone who is only working on low priority incidents. I also think that the how, when, what, who and recommendation are useful when it comes to incident analysis and helped during my analysis.

Participant P3

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ○ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ◉ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

2 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

.....

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

.....

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

From what I have done in this assessment, the criteria for quality analysis allowed me to understand a more comprehensive and procedural process of analyzing events.

It also showed me the area that still need to improve from the 7 step of incident analysis processes.

Participant P4

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- (●) SOC Manager
- ( ) SOC Analyst
- ( ) Other: .....

2. Which industry do you work in? *

- ( ) Information Technology
- ( ) Airline and Aerospace
- ( ) Defence
- ( ) Banking and Finance
- ( ) Construction and Transportation
- (●) Managed Security Service Provider (MSSP)
- ( ) Health and Social Care
- ( ) Telecommunication
- ( ) Other: .....

3. How many years of SOC experience do you have? *

10 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

Helps the Manager, and the analyst to see the strong and weak points of how they are working which can lead to the improvements needed.

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

I think the SOC-AAM helps validate your perceived performance off the Analyst which allows you to look at the impacting factors around what could be the cause of those results. Without the SOC-AMM, it is sometimes hard to gauge the overall performance so you are just picking up on maybe a few points instead.

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

Participant P5

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

5 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I found using the SOC-AMM guidelines useful as it streamlined my work focus which in my opinion made me much more efficient. Overall, I think the tool improved my performance.

Participant P6

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

3 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I think it made it easier to rate my overall performance in terms of the functions listed on the SOC-AAM. I also think that the guidelines provided by the SOC-AAM made is easier when analysing packets. So, I will say that it had a positive impact on my performance.

Participant P7

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

5 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

Overall, I think the SOC-AAM is a good and a simple tool to use. I like the way it breaks down the different functions so I can easily see the areas that I did well.

Participant P8

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

4 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

Even though log analysis is not something new to me, I found the criteria that you have for assessing the quality of analysis really useful. In my opinion, those criteria definitely had some impact on my thinking process.

Participant P9

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

8 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	○	◉

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

.....

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

.....

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

The SOC-AAM did not improve my performance in terms of what is expected of me as an analyst.

Participant P10

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

6 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	◉	○	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	◉	○	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

While it felt satisfying knowing exactly what I am being assessed on, my concern is that there are still a number of things that takes a lot of my time that is not reflected in the SOC-AAM. For example, replying to emails and responding to phone calls.

Participant P11

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

1 year

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	○	◉
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I think the SOC-AAM is useful, especially the who, when , how, what criteria which I believed helped my thinking process and showed me how to take in a lot of information from an incident and organise them in concise steps when writing my report.

Participant P12

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

4 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	◉	○	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

In my opinion, although I found the SOC-AMM easy to use, I still think that when I am being asked to work on things that are not in the SOC-AAM I wouldn't achieve any score, but to be fair, it covers all the major functions we are expected to do and would say it improved my performance in the areas I am being measured on.

Participant P13

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: _____

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: _____

3. How many years of SOC experience do you have? *

3 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

In my opinion, the guidelines included in the SOC-AAM helped me to improve on the kind of information that I would have normally included in my report.

Participant P14

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

4 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	○	◉
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	○	◉
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	○	◉

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

The SOC-AAM has helped me to improve my performance as I know the tasks I am being assessed on. The criteria for quality analysis brings everything together nicely.

Participant P15

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- (●) SOC Manager
- ( ) SOC Analyst
- ( ) Other: .....

2. Which industry do you work in? *

- ( ) Information Technology
- ( ) Airline and Aerospace
- ( ) Defence
- ( ) Banking and Finance
- ( ) Construction and Transportation
- (●) Managed Security Service Provider (MSSP)
- ( ) Health and Social Care
- ( ) Telecommunication
- ( ) Other: .....

3. How many years of SOC experience do you have? *

11 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	◉	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	◉	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

This is the first time we have used something like this to evaluate performance in our SOC. I think it is fair to say that all the analysts gave a good account of themselves. Overall, I believe that the SOC-AAM is a helpful tool for evaluating analysts performance and pleased with the approach. The guidelines for assessing the quality of analysts analysis has been useful to the team. I think it encouraged them to expand their thinking and take a step back to think through what they need to do when writing their incident report. I also believe that the tool made it possible for everyone within the team to understand the basis upon which they are being assessed.

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

There are some competitive individuals within the team, so I was expecting those individuals to show that competitiveness. However, looking at the monthly scores, it was great to see that all the analysts did pretty well. I am of the opinion that the scores achieved by each individual analyst reflected in how I perceive their contribution to the team. One area that I saw improvement across the board is report writing.

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

Participant P16

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

5 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	◉	○
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	◉	○
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	◉	○	○

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	◉	○
Overall, I found the SOC-AAM easy to use.	○	○	◉	○	○
I found the SOC-AAM easy to learn.	○	○	○	◉	○
The SOC-AAM is clear and easy to grasp.	○	○	○	◉	○

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	◉	○	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	◉	○	○
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	◉	○	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I actually think that having this tool is good but it takes a lot of time to fill this form with all these statistics especially when we are busy. Maybe if it can be incorporated into our ticketing system it will be much better. As to whether it improved by performance or not, it is hard to say to be honest.

Participant P17

The SOC-AAM: Post Testing Questionnaire -v2

1. What is your role title in your organisation? *

- ○ SOC Manager
- ◉ SOC Analyst
- ○ Other: .....

2. Which industry do you work in? *

- ○ Information Technology
- ○ Airline and Aerospace
- ○ Defence
- ○ Banking and Finance
- ○ Construction and Transportation
- ◉ Managed Security Service Provider (MSSP)
- ○ Health and Social Care
- ○ Telecommunication
- ○ Other: .....

3. How many years of SOC experience do you have? *

2 years

4. Perceived Usefulness (PU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	○	○	○	○	◉
I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	○	○	○	○	◉
The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	○	○	○	○	◉

5. Perceived Ease of Use (PEOU) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the procedure for applying the SOC-AAM easy to follow.	○	○	○	○	◉
Overall, I found the SOC-AAM easy to use.	○	○	○	◉	○
I found the SOC-AAM easy to learn.	○	○	○	○	◉
The SOC-AAM is clear and easy to grasp.	○	○	○	○	◉

6. Intention to Use (ItU) the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	○	○	○	◉	○
In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	○	○	○	◉	○
I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	○	○	○	◉	○

7. Perceived Completeness (PCO) of the SOC-AAM *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance	○	○	○	○	◉
I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	○	○	○	◉	○

Managers Only

8. In your opinion, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance, or did it not make any difference to their performance? *

9. In your opinion, did the performance score(s) of your analysts when using the SOC-AAM as the evaluation tool reflect your perceived performance of each analyst within your team? *

Analysts Only

In your opinion, did the introduction of the SOC-AAM lead to an improvement in your performance, or did it not make any difference to your performance?

I think my performance remained the same but I found the guidelines interesting and useful.

M Survey Results

Table 59: Participants responses to the MAM survey

Question	PU1	PU2	PU3	PEOU1	PEOU2	PEOU3	PEOU4	ItU1	ItU2	ItU3	PCO1	PCO2
Participant 1	5	4	4	4	5	5	5	5	5	5	4	5
Participant 2	5	4	4	5	5	5	5	5	5	5	5	5
Participant 3	5	5	5	5	5	5	5	5	5	5	5	5
Participant 4	4	4	4	4	5	5	4	4	5	5	4	5
Participant 5	4	4	4	4	4	4	4	5	5	5	5	5
Participant 6	5	5	5	5	5	5	5	5	5	5	5	4
Participant 7	5	5	5	4	4	5	5	4	4	4	5	5
Participant 8	4	5	5	5	5	4	5	4	4	5	4	4
Participant 9	5	5	5	5	5	5	5	4	4	4	5	5
Participant 10	5	5	5	5	5	5	5	3	4	4	3	4
Participant 11	5	5	5	5	5	5	5	5	5	5	4	4
Participant 12	4	4	4	4	4	4	4	4	5	4	3	4
Participant 13	4	4	4	4	4	4	4	5	5	5	4	4
Participant 14	4	4	4	4	4	4	4	5	5	5	4	4
Participant 15	4	4	3	4	3	4	4	3	4	4	3	3
Participant 16	5	5	5	5	4	5	5	4	4	4	5	4
Participant 17	4	4	4	4	4	4	4	4	4	4	4	4

Assigned scores: Strongly Disagree -1; Disagree - 2; Neutral - 3; Agree -4; Strongly Agree - 5.

Table 60: Perceived Usefulness: Number of respondents by the answers provided

Answer/Item	PU1	PU2	PU3
Strongly Agree (5)	9	8	8
Agree (4)	8	9	8
Neutral (3)	0	0	1
Disagree (2)	0	0	0
Strongly Disagree (1)	0	0	0

Table 61: Perceived Ease of Use: Number of respondents by the answers provided.

Answer/Item	PEOU1	PEOU2	PEOU3	PEOU4
Strongly Agree (5)	8	9	10	10
Agree (4)	9	7	7	7
Neutral (3)	0	1	0	0
Disagree (2)	0	0	0	0
Strongly Disagree (1)	0	0	0	0

Table 62: Intention to Use: Number of respondents by the answers provided

Answer/Item	ItU1	ItU2	ItU3
Strongly Agree (5)	8	10	10
Agree (4)	7	7	7
Neutral (3)	2	0	0
Disagree (2)	0	0	0
Strongly Disagree (1)	0	0	0

Table 63: Perceived Completeness: Number of respondents by the answers provided.

Answer/Item	PCO1	PCO2
Strongly Agree (5)	7	7
Agree (4)	7	9
Neutral (3)	3	1
Disagree (2)	0	0
Strongly Disagree (1)	0	0

Table 64: The descriptive statistics for the Survey data

Question	Median	Mean	Std. Dev
PU	4	4.4706	0.54233
PEOU	5	4.5294	0.53170
ItU	5	4.5098	0.57871
PCO	4	4.2941	0.67552

N Ethical Approval

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

Instructions

Do not use this form if your research is with the NHS or NHS-linked: please refer instead to the NHS Local Research Ethics Committee.

Do not use this form if your research involves adults who do not have the capacity to consent. Such projects have to be submitted to the National Research Ethics Service (NRES) system: http://nres.nhs.uk/

Please carefully review:

- School Research Ethics documentation
- Data management, collecting personal data, data protection act requirements
- Information Security Framework
- Research Integrity and Governance
- Research Ethics

Please complete the Research Integrity Online Training Programme (Staff link, Student link) prior to submitting this form.

Please complete this form at least **2 weeks** before starting your data collection/human involvement activities and send to comsc-ethics@cardiff.ac.uk along with **all** the relevant attachments:

- Full Project plan/proposal
- Participant Information Form, either:
  - hard copy, e.g briefing and debriefing (if appropriate)
  - online equivalent
- Consent Form or online equivalent (or justification as to why this is not possible)
- Certificate(s) of completion of the Research Integrity Online Training Programme (RIOTP) for all staff associated with a project (and students if applicable).
- (If applicable) Details concerning external funding
- (If an extension is requested) Provide a list of motivations and list of amendments to any previous approvals

Submissions will be reviewed at the next COMSC Research Ethics Group meeting held approximately fortnightly.

Page 1 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

1 General Information

Title of Project:

A Framework for Evaluating the Performance of Cyber Security Operations Centre Analysts

If this submission relates to a previous approval request (e.g. a revision or extension):

Previous ID:

If this approval refers to an Undergraduate or Masters Student Project:

Student(s) Names and IDs:

Supervisor Name(s):

If this approval refers to a research project (e.g. Staff, Postgraduate Research Student):

Principle Researcher: Enoch Agyepong

Other Researchers:

Project Start Date: 01.10.18 — End Date: 01.10.25

Attachments:	Yes	NA	Document Version ID
Full project plan/proposal	X		
Participant Information Form	X		
Consent Form	X		
RIOTP Completion Certificates	X		
Details concerning external funding		X	
Motivations for and list of amendments		X	

Page 2 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

2 Recruitment Procedure

		Yes	No	NA
1	Does your project include children under 18 years of age?	☐	☒	☐
	If "Yes," have you read and understood Cardiff University's Code of Practice for researchers Working With Children and Young People which forms part of the Safeguarding Children and Vulnerable Adults Policy? The Interim Guidance is at Appendix 1, Page 9 of this Policy	☐	☐	
2	Does your project include people with learning or communication difficulties?	☐	☒	☐
3	Does your project include people in custody?	☐	☒	☐
4	Is your project likely to include people involved in illegal activities?	☐	☒	☐
5	Does your project involve people belonging to a vulnerable group, other than those listed above?	☐	☒	☐
6	Does your project include people who are, or are likely to become your clients or clients of the department in which you work?	☐	☒	☐
7	Does your project provide for people for whom English / Welsh is not their first language?	☐	☒	☐

If any of the blue boxes has been ticked, please explain how the potential ethical issue(s) will be handled:

Please describe how do you plan to recruit participants:

The researcher will use personal contact from the cybersecurity industry to recruit the initial set of analysts and SOC managers for the study. Participating analysts and SOC managers will be requested to recommend colleagues with relevant SOC experience who might be interested in this study, under a snowballing process. In all cases, interested participants will be given the participant information form and a consent form.

Page 3 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

3 Consent Procedures

		Yes	No	NA
8	Will you tell participants that their participation is voluntary?	☒	☐	
9	Will you obtain written consent for participation?	☒	☐	
10	If the research is observational, will you ask participants for their consent to being observed?		☐	☒
11	Will you tell participants that they may withdraw from the research at any time and for any reason?	☒	☐	
12	Will you give potential participants a significant period of time to consider participation?	☒	☐	

If any of the blue boxes has been ticked, please explain how the potential ethical issue(s) will be handled:

Page 4 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

4 Possible Harm to Participants

		Yes	No	NA
13	Is there any realistic risk of any participants experiencing either physical or psychological distress or discomfort?	☐	☒	☐
14	Is there any realistic risk of any participants experiencing a detriment to their interests as a result of participation?	☐	☒	☐

If any of the blue boxes has been ticked, please explain how the potential ethical issue(s) will be handled:

Not Applicable

If there are any risks to the participants, please explain how you intend to minimise these risks:

Not Applicable

Page 5 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

5 Data Protection

		Yes	No	NA
15	Will any non-anonymised and/or personalised data be generated and/or stored?	☒	☐	☐
16	Will you have access to documents containing sensitive data about living individuals?	☐	☒	☐
	If "Yes" will you gain the consent of the individuals concerned	☐	☐	
17	Are you planning to use Cardiff University installation of OneDrive to store data	☐	☒	☐
	If "No" is your data storage policy compliant with Cardiff University ISF	☒	☐	☐

Sensitive data are inter alia data that relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, actual and alleged offences.

Please describe how you will securely collect and store any data (**required**):

The data for this study will be collected through interviews and focus group sessions.
All participants will be asked to read and sign the consent form associated with this study. The signed consent forms along with the interview notes will be stored securely in a lockable room. Electronic data will be stored on the university's encrypted laptop and on a password protected recording device.

The data from the interviews and the focus group sessions will be kept for 6 years upon completion of the research as per the university's policy for non-clinical research.

All the data forms will be destroyed using shredder once the allowed retention period is over.

If any of the blue boxes have been ticked, please explain how the potential ethical issue(s) will be handled:

Not Applicable

Page 6 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

6 Researcher Safety

		Yes	No	NA
18	If relevant to your research, have you taken into account the Cardiff University guidance on safety in fieldwork / for lone workers?	☒	☐	☐

If any of the blue boxes have been ticked, please explain how the potential ethical issue(s) will be handled:

Page 7 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

7 Researcher Governance

		Yes	No	NA
19	Does your study include the use of a drug? You will need to contact Research Governance before submission (resgov@cf.ac.uk)	☐	☒	☐
20	Does the study involve the collection or use of human tissue? You will need to contact the Human Tissue Act team before submission (hta@cf.ac.uk)	☐	☒	☐

If any of the blue boxes have been ticked, please explain how the potential ethical issue(s) will be handled and please attach approvals received from Research Governance and/or Human Tissue Act team:

Page 8 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

8 Prevent Duty

		Yes	No	NA
21	Has due regard been given to Prevent duty, in particular to prevent anyone being drawn into terrorism? Prevent Duty Guidance Procedure Freedom of Speech	☐	☐	☒

If any of the blue boxes have been ticked, please explain how the potential ethical issue will be handled:

Page 9 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

9 Other Ethical Considerations

If there are other potential ethical issues that you think the Committee should consider please explain them in the following space. It is your obligation to bring to the attention of the Committee any ethical issues not covered on this form.

Page 10 of 11

APPROVED
Approval ID: COMSC/Ethics/2019/063

School of Computer Science & Informatics

Ethical Approval Request Form
Form valid until 15th November 2019

10 Any other comments

If there is additional information that you think the Committee should consider please explain in the space below:

Page 11 of 11

O Interviews - Participants' Briefing Sheet and Consent Form

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

A Framework for Evaluating the Performance of Cyber Security Operations Centre Analysts

Participant Information Sheet

Introduction

You are being invited to take part in a research study. Before you decide, it is important for you to understand why the research is being done and what this study entails. Please take the time to read this information sheet carefully. If there is anything that is not clear or if you would like more information, please ask. Also, take time to decide whether or not you want to take part. Thank you for reading this.

What is the purpose of the study?

The purpose of this study is to investigate metrics and measures for assessing the performance of analysts working in a Security Operations Centre (SOC). This will help to design a comprehensive framework that can be used to evaluate the performance of analysts working in SOCs offering different functions. Additionally, this study will also seek to investigate human factors that impact on the performance of analysts along with measurement methods for assessing the identified human factors.

How is the study structured?

Once you have agreed to take part in the study, you will be asked to take part in a one-to-one in-depth interview that should take less than 1 hour. The purpose of the interview is to obtain your opinion and feedback on an initial framework that can be drawn on to evaluate the performance of analysts. Your feedback and input will be used to improve the initial framework. Please feel free to ask questions regarding this study at any time.

Why have I been chosen?

You have been chosen because as a someone with SOC work experience, you have knowledge and opinion on how the performance of analysts can be captured and measured. You may also have knowledge of some of the human factors that impact on the performance of analysts that you can share with the researcher.

Do I have to take part?

It is up to you to decide whether or not you want to take part in the study. If you do decide to take part, you will be asked to sign a consent form. Please note that, if you choose to take part in this study, you are still free to withdraw at any time and without giving a reason.

Are there any benefits in taking part?

Given that this research seeks to uncover a real-life account on how the performance of analysts can be measured, your participation will contribute towards the designing of a comprehensive framework for evaluating the performance of analysts. The final proposed framework will also be shared freely with you.

How will the data be collected and stored?

The interview will be taped recorded because I do not want to miss any information. Also, I will write down some notes during the interview. All the information that is collected from you will be kept strictly confidential and will only be made available to the research supervisory team.

The interview data will be kept for six years upon completion of the research as per Cardiff University's Policy on data storage for non-clinical research. The data forms will be destroyed using shredder once the allowed retention period is over. Electronic data will be stored on the University an encrypted laptop and will be password protected. Besides, any output published using the data collected will be anonymised to ensure that, it is not possible for other people to know your name or identify you in any way.

How can I request access to my data?

You have the right to request access to the data you provided as part of this study. You can access this right by notifying the principal investigator, Enoch Agyepong either verbally or in writing.

What if I want to end my participation in this study?

If you want to stop your participation for any reason, you may do so by informing me at any stage during the interview process.

What will happen to the results of the research study?

Where appropriate, the results of this study will be published. However, you will not be identified in any report or publication. We will inform you of the results of the study if you wish to have the information.

What do I do if I have any complaints regarding this study?

If you have any concerns regarding this study, please speak to the Principal Investigator [Enoch Agyepong], who will do his best to address your concerns. If you remain unhappy please contact the main supervisor for this research study: Dr Yulia Cherdansteva or the Research Ethics Committee:

Cardiff School of Computer Science & Informatics Ethics Committee
Email: comsc-ethics@cardiff.ac.uk

The data controller is Cardiff University and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

Who has reviewed the study?

This study has been reviewed and approved by the Ethics Committee of the School of Computer Science and Informatics, Cardiff University. Ethics application number: [COMSC/Ethics/2019/063].

Contact for Further Information

We welcome the opportunity to answer any question you may have about any aspect of this study or your participation in it. Please contact

Enoch Agyepong

School of Computer Science and Informatics

Tel. No.: +447852951615

Email: agyeponge@cardiff.ac.uk

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

A Framework for Evaluating the Performance of Cyber Security Operations Centre Analysts
Participant Consent Form

Name of participant/identifier: _____

Please read the participant information sheet and then read the following statements carefully before signing this form. If you have any questions, please feel free to ask me (Enoch Agyepong). You are under no pressure to give your consent, and you are free to withdraw from this study at any time. If you have any complaints or concerns about this study, please contact comsc-ethics@cardiff.ac.uk. The data controller is Cardiff University, and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

By adding your initials in the box to the right of each item and signing the form at the bottom, you are agreeing to the following:

	INITIALS
1. I confirm that I have read and understood the Participant Information Sheet for this study and I have had the opportunity to ask questions about it.	
2. I understand that participation in this study is entirely voluntary and that I can withdraw from the study at any time without giving a reason, and without any consequences.	
3. I understand how to raise a concern or make a complaint.	
4. I consent to being audio recorded during the interview	
5. I also understand that the audio recording and any note taken during the interview will be anonymised and used in the research output.	
6. I understand that the research data collected will be held confidentially, such that only the researchers can trace this information back to me individually. The data will be retained for up to 6 years when it will be deleted/destroyed.	
7. I understand that I can ask for the information I provide to be deleted/destroyed at any time.	
8. I agree to take part in the following study.	

I, _____ consent to participate in the study conducted by [INSERT], School of Computer Science, Cardiff University.

Signed: Date:

P Delphi Study - Participants' Briefing Sheet and Consent Form

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

Evaluating the Performance of Cyber Security Operations Centre Analysts: A Delphi Study

Participant Information Sheet

Introduction

You are being asked to participate in a Delphi study, which is a systematic approach for obtaining consensus on the opinions of 'experts', through a series of structured questionnaires. The Delphi process will consist of two to three rounds of questionnaires. As part of the Delphi process, the responses from each round will be fed back in summarised form to the participants, who are then given an opportunity to respond again to the emerging data.

What is the purpose of the study?

The purpose of this study is to assign weights to the tasks expected of an analyst and also to gather experts' opinion regarding the criteria for evaluating the quality of analysis and quality of an analyst's report. This will help to design a framework for evaluating the performance of analysts based on their task performance.

How is the study structured?

Once you have agreed to take part in the study, you will be requested to complete the attached spreadsheet as part of the ***first round*** of the Delphi process. The attached video demonstrates the process for completing the spreadsheet. Participants are required to send their completed spreadsheet by email to the researcher within two weeks of receiving this email. The deadline for returning the form for the first round is **Friday 14th August 2020**.

Participants will be provided with feedback on the findings obtained from the group within two weeks of returning the spreadsheet for *round one*. The feedback would provide participants with the opportunity to reconsider their decision in light of the consolidated findings from the group.

Participants would have the choice to reconsider their initial responses in *round two*. Participants can either adjust or maintain the findings from the group before returning the completed form to the researcher during *round two*. The deadline for returning the form for the ***second round*** will be

communicated to all participants when the feedback is provided for round one. If there is a consensus during *round two*, the Delphi process will cease. Where there is no consensus, *a third* and *final round* would be conducted. The timings and the deadline for the third round (if required) will be communicated to participants in the round two feedback. Each round would take approximately 30 minutes to complete.

Why have I been chosen?

You have been chosen because, as someone with SOC work experience, you have knowledge and opinions on how the performance of analysts can be measured. You may also have knowledge of criteria that can be used to access the quality of an analyst's analysis and quality of their report.

Do I have to take part?

It is up to you to decide whether or not you want to take part in the study. If you do decide to take part, you will be asked to sign a consent form. Please note that, if you choose to take part in this study, you are still free to withdraw at any time and without giving a reason.

Are there any benefits in taking part?

Given that this research seeks to uncover a real-life account on how the performance of analysts can be measured, your participation will contribute towards the designing of a comprehensive framework for evaluating the performance of analysts. The final proposed framework will also be shared freely with you.

How will the data be collected and stored?

All the information that is collected from you will be kept strictly confidential and will only be made available to the supervisory team. The data will be kept for six years upon completion of the research as per Cardiff University's Policy on data storage for non-clinical research. The data forms will be destroyed using a shredder once the allowed retention period is over. Electronic data will be stored on a University encrypted laptop and will be password protected. In addition, any output published using the data collected will be anonymised to ensure that it is not possible for other people to know your name or identify you in any way.

How can I request access to my data?

You have the right to request access to the data you provided as part of this study. You can access this right by notifying the principal investigator, Enoch Agyepong, either verbally or in writing.

What will happen to the results of the research study?

Where appropriate, the results of this study will be published. However, you will not be identified in any report or publication. We will inform you of the results of the study if you wish to have the information.

What do I do if I have any complaints regarding this study?

If you have any concerns regarding this study, please speak to the Principal Investigator [Enoch Agyepong], who will do his best to address your concerns. If you remain unhappy, please contact the main supervisor for this research study: Dr Yulia Cherdansteva or the Research Ethics Committee:

Cardiff School of Computer Science & Informatics Ethics Committee
Email: comsc-ethics@cardiff.ac.uk

The data controller is Cardiff University and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

Who has reviewed the study?

This study has been reviewed and approved by the Ethics Committee of the School of Computer Science and Informatics, Cardiff University. Ethics application number: [COMSC/Ethics/2019/063].

Contact for Further Information

We welcome the opportunity to answer any question you may have about any aspect of this study or your participation in it. Please contact:

Enoch Agyepong
School of Computer Science and Informatics
Tel. No.: +447852951615
Email: agyeponge@cardiff.ac.uk

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

Evaluating the Performance of a Security Operation Centre Analysts: A Delphi Study

Consent Form

Name of participant/identifier: _____

Please read the participant information sheet and then read the following statements carefully before signing this form. If you have any questions, please feel free to ask me (Enoch Agyepong). You are under no pressure to give your consent, and you are free to withdraw from this study at any time. If you have any complaints or concerns about this study, please contact comsc-ethics@cardiff.ac.uk. Thedata controller is Cardiff University, and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

By adding your initials in the box to the right of each item and signing the form at the bottom, you are agreeing to the following:

	INITIALS
1. I confirm that I have read and understood the Participant Information Sheet for this study and I have had the opportunity to ask questions about it.	
2. I understand that participation in this study is entirely voluntary and that I can withdraw from the study at any time without giving a reason and without any consequences.	
3. I understand how to raise a concern or make a complaint.	
4. I give permission for my anonymised responses to be used during the Delphi process and to be accessed by members of the research supervisory team. I understand that my name will not be linked with the research materials and I will not be identifiable during the Delphi survey or in the reports that result from the research.	
5. I understand that the research data collected will be held confidentially, such that only the researchers can trace this information back to me individually. The data will be retained for up to 6 years, when it will be deleted/destroyed.	
6. I understand that I can ask for the information I provide to be deleted/destroyed at any time.	
7. I agree to take part in the following study.	

I,_____consent to participate in the study conducted by [INSERT], School of Computer Science, Cardiff University.

Signed: Date:

Completion: Please return scanned or electronically completed forms via email to: agyeponge@cardiff.ac.uk.
Please retain a copy of the completed consent form for your personal records.

Q SOC-AAM Testing: Participants' Briefing Sheet and Consent Form

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

Measuring the Performance of a Security Operations Centre Analyst

Participant Information Sheet

Introduction

I would like to invite you to take part in a research project to test a new method for measuring the performance of an analyst. Before you decide you need to understand why the research is being done and what it will involve you. Please take the time to read the following information carefully and ask questions about anything you do not understand.

What is the purpose of the study?

The purpose of this study is to test and evaluate a new method for measuring the performance of an analyst designed as a result of this study.

How is the study structured?

Once you have agreed to take part in the study, you will be requested to complete the performance assessment tool. The tool comes with a step-by-step instruction on its usage.

Participants will be provided with a survey upon the completion of the testing to provide their feedback on the new method.

Why have I been chosen?

You have been chosen because the designed method is solely for the purposes of assessing an analyst's performance and as an analyst you are best placed to assess the usefulness of the new method.

Do I have to take part?

It is up to you to decide whether or not you want to take part in the study. If you do decide to take part, you will be asked to sign a consent form. Please note that, if you choose to take part in this study, you are still free to withdraw at any time and without giving a reason.

Are there any benefits in taking part?

Participants in this study could freely request the final version of the designed method for their use.

How will the data be collected and stored?

All the information that is collected from you will be kept strictly confidential and will only be made available to the supervisory team. The data will be kept for six years upon completion of the research as per Cardiff University's Policy on data storage for non-clinical research. The data forms will be destroyed using a shredder once the allowed retention period is over. Electronic data will be stored on a university encrypted laptop and will be password protected. In addition, any output published using the data collected will be anonymised to ensure that it is not possible for other people to know your name or identify you in any way.

How can I request access to my data?

You have the right to request access to the data you provided as part of this study. You can access this right by notifying the principal investigator, Enoch Agyepong, either verbally or in writing.

What will happen to the results of the research study?

Where appropriate, the results of this study will be published. However, you will not be identified in any report or publication. We will inform you of the results of the study if you wish to have the information.

What do I do if I have any complaints regarding this study?

If you have any concerns regarding this study, please speak to the Principal Investigator [Enoch Agyepong], who will do his best to address your concerns. If you remain unhappy, please contact the main supervisor for this research study: Dr Yulia Cherdansteva or the Research Ethics Committee:

Cardiff School of Computer Science & Informatics Ethics Committee
Email: comsc-ethics@cardiff.ac.uk

The data controller is Cardiff University and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

Who has reviewed the study?

This study has been reviewed and approved by the Ethics Committee of the School of Computer Science and Informatics, Cardiff University. Ethics application number: [COMSC/Ethics/2019/063].

Contact for Further Information

We welcome the opportunity to answer any question you may have about any aspect of this study or your participation in it. Please contact:

Enoch Agyepong
School of Computer Science and Informatics
Tel. No.: +447852951615
Email: agyeponge@cardiff.ac.uk

School of Computer Science and Informatics
Enoch Agyepong (Principal Investigator)
+44(0)7852951615
agyeponge@cardiff.ac.uk
Dr Yulia Cherdantseva (Main Supervisor)
cherdantsevayv@cardiff.ac.uk

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

Measuring the Performance of a Security Operation Centre Analyst

Consent Form

Name of participant/identifier: _____

Please read the participant information sheet and then read the following statements carefully before signing this form. If you have any questions, please feel free to ask me (Enoch Agyepong). You are under no pressure to give your consent, and you are free to withdraw from this study at any time. If you have any complaints or concerns about this study, please contact comsc-ethics@cardiff.ac.uk. The data controller is Cardiff University, and the Data Protection Officer is Matt Cooper CooperM1@cardiff.ac.uk. The lawful basis for the processing of the data you provide is consent.

By adding your initials in the box to the right of each item and signing the form at the bottom, you are agreeing to the following:

	INITIALS
1. I confirm that I have read and understood the Participant Information Sheet for this study, and I have had the opportunity to ask questions about it.	
2. I understand that participation in this study is entirely voluntary and that I can withdraw from the study at any time without giving a reason and without any consequences.	
3. I understand how to raise a concern or make a complaint.	
4. I give permission for my anonymised responses to be used in this study and to be accessed by members of the research supervisory team. I understand that my name will not be linked with the research materials, and I will not be identifiable during the study or in the reports that result from the research.	
5. I understand that the research data collected will be held confidentially, such that only the researchers can trace this information back to me individually. The data will be retained for up to 6 years, when it will be deleted/destroyed.	
6. I understand that I can ask for the information I provide to be deleted/destroyed at any time.	
7. I agree to take part in the following study.	

I,_____consent to participate in the study conducted by [INSERT], School of Computer Science, Cardiff University.

Signed: Date:

Completion: Please return scanned or electronically completed forms via email to: agyeponge@cardiff.ac.uk.
Please retain a copy of the completed consent form for your personal records.

Glossary

Advanced Persistent Threat (APT) - A stealthy, sophisticated hacking attack against a specific network or system, usually intended to steal data or assets.

Alert - A notification from your computer systems.

Anti-Virus - Software which scans the files going in and out of your computer systems and tries to spot hidden software that is designed to cause damage or theft of data.

Asset - Is any piece of information, software or hardware that an organisation uses in the course of its business activities.

CIA - Confidentiality, Integrity and Availability: the three core pillars of cybersecurity.

Computer Incident Response Team (CIRT) - A team that exists to provide response and recovery from a computer or cyber security incident.

Cyber Security Incident Response Team (CSIRT) - Synonymous with a CIRT.

Cyber Security Operation Centre (CSOC) - Synonymous with a SOC.

Design Science Research (DSR) - A problem-solving research strategy that seeks to enhance human knowledge through the creation of new and innovative artefacts.

Event - An action initiated by the user or the computer system.

False Negative - Denotes a situation, where no alert is raised when an attack has occurred.

False Positive - Denotes a non-malicious security event or an alert that is reported as malicious by a security reporting tool.

Firewall - A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted).

Hardening - Taking a default installation of a computer system and changing its configuration to make it more secure - by disabling unnecessary or unused system components.

Incident - An alert that is not part of standard operations or normal expected activity and could cause loss or harm.

Intrusion Detection System (IDS) - A hardware or software tool that monitors a network or system for malicious activity.

Intrusion Prevention System (IPS) - Similar to an IDS but has extra features that can take action to attempt to stop the attack.

Key Performance Indicator (KPI) - A measurable value that demonstrates how well a person or a company achieves key business objectives.

Managed Security Service Provider (MSSP) - An organisation that provides outsourcing security operations centre services to multiple clients.

Measure - A quantifiable, observable, and objective data supporting a metric. It is a number that can be used in calculations, such as summation, counting, or averaging.

Method Adoption Model (MAM) - A theoretical model for validating information System Design Methods derived from the MEM.

Method Evaluation Model (MEM) - A theoretical model for validating information System Design Methods.

Metric - A quantifiable measure that is used to track and assess performance. A metric is derived from one or more measures.

Network Operations Centre (NOC) - A centralised location where IT teams monitor the performance and health status of a network and IT systems.

Patch - A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.

Patch Management - Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application.

Penetration Testing - A systematic process of simulating a cyberattack against an organisation to identify vulnerabilities in their networks and applications.

Security Information and Event Management (SIEM) - A system that collates log and event data received from a wide variety of systems and reports perceived issues to the security operations team.

Security Operations Centre (SOC) - A centralised location inside or outside an organisation that monitors an organisation's security operations to prevent, detect and respond to any potential threats.

Security Operations Centre Analysts Assessment Framework (SOC-AAF) - A framework for understanding the core functions of an analyst and metrics for measuring their performance.

Security Operations Centre Analysts Assessment Method (SOC-AAM) - A method for measuring the performance of an analyst in a systematic manner.

Service Level Agreement (SLA) - An agreement between a supplier and a customer that forms a framework for the provision of the services, often including security-specific requirements.

Small and medium-sized Enterprises (SMEs) - Businesses whose personnel and revenue numbers fall below certain limits.

Threat - A situation or event that could possibly have an adverse effect on a computer system, but which has yet to occur.

True Negative - An event when no attack has occurred and no detection is made.

True Positive - A legitimate attack which triggers an alert.

Vulnerability - Refers to a flaw in a system that can leave it open to attack.

Zero Day Attack - Attacks that exploit a vulnerability in software that is unknown to the vendor and has no remediation available.