Towards a Framework for Measuring the Performance of a Security Operations Center Analyst

[Cyber Security 2020]

Enoch Agyepong
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
agyeponge@cardiff.ac.uk

Yulia Cherdantseva
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
cherdantsevayv@cardiff.ac.uk

Philipp Reinecke
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
reineckep@cardiff.ac.uk

Pete Burnap
School of Computer Science and Informatics
Cardiff University
Cardiff, UK
p.burnap@cs.cardiff.ac.uk

***Abstract*—The past few years have seen several studies reporting on the role of a Security Operations Center (SOC) analyst and metrics for assessing the performance of analysts. However, research suggests that analysts are dissatisfied with existing metrics as they fail to take into consideration several aspects of their tasks. Existing works advocate for research into this area. A major challenge to devising adequate metrics is that the real work of analysts that needs to be taken into consideration to assess their holistic performance has not been fully discussed. Furthermore, at present, there is no agreement on what constitutes core analysts' functions. Analysts' overall performance in a SOC could be obtained if there is a common agreement on the core functions upon which their performance can be evaluated. In this paper, we propose a framework depicting the core functions of analysts and KPIs that can be used to measure the performance of analysts. To do this, we conducted a thorough analysis of 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. Our research results identify the following: *quality of analysts' analysis, quality of analysts' report, time-based measures* and the *absolute numbers derived from an analyst's tasks* as the key performance indicators (KPIs) for assessing analysts' performance. We hope that our findings will stimulate more interest among cybersecurity researchers on assessment methods for analysts.**

Keywords— Security Operations Center, Analysts' Functions, Analysts' Metrics, Performance Metrics, Key Performance Indicator

I. INTRODUCTION

Cybersecurity incidents and attacks usually cause severe financial and reputational damage to organisations. For example, a report by the UK's Department of Health in 2018 indicates that the WannaCry ransomware cost the National Health Service (NHS) roughly £92 million [1]. To detect malicious activities and to reduce the damage caused by cybercriminals, organisations typically rely on several preventative and defensive strategies [2]. Amongst these strategies is the use of a security operations center (SOC). A SOC is a centralized location inside or outside an organisation comprising of a specialized team of IT professionals that support businesses to deal with cybersecurity incidents [3].

SOCs are being used by both private and public sector organisations to monitor their enterprise network, to detect attacks, respond to cyber threats and address incident management activities [4]. The growing use of SOCs has led to several studies on SOCs and their operations [5]–[8]. Despite being a widely researched topic, there are some aspects of SOCs that have still not been adequately addressed [4], [9]. Areas that have not been adequately addressed include adequate metrics for SOC analysts; the factors that need to be taken into consideration when evaluating effort of analysts holistically; and strategies for addressing the challenges faced by analysts [4], [9]–[11].

Although there have been some suggestions from cybersecurity researchers and writers on the role of analysts [12], [13], along with some metrics for assessing their performance, the emerging consensus amongst researchers is that there is a need to improve metrics for the analysts [4], [8], [9]. In fact, an anthropological study conducted by Sundaramurthy et al. [14] found that analysts are particularly dissatisfied with existing metrics as they fail to take into consideration several aspects of their functions. The literature also suggests that the lack of adequate assessment method causes frustration for both analysts and SOC managers [14]. Despite this problem, there are very few attempts from researchers to investigate how existing metrics for the analysts can be improved, or the main factors that should be taken into consideration when assessing the performance of analysts.

An objective of this paper is to contribute towards filling the current gap in the literature on the absence of clear understanding of key functions of a SOC analyst and of the factors/criteria that should be taken into consideration to evaluate analysts' performance. It is our contention that the lack of a clear delineation of analysts' functions within a SOC contributes to the present problem. Our proposition is that, by focusing on the daily tasks and functions of an analyst, a framework can be developed that highlights the aspects of analysts' operations that should be used to assess their holistic performance.

In this paper, we propose a framework on the main functions of analysts in a SOC along with the key factors that should be taken into consideration by SOC stakeholders and cybersecurity researchers when assessing the performance of analysts. Dafikpaku [15] defines a framework as an outline or overview of interlinked items/activities built to facilitate an approach towards achieving a specific goal. Drawing on this understanding, we present an overview and an outline of analysts' functions and criteria by which analysts can be assessed using a framework to facilitate our goal towards designing a comprehensive approach for evaluating analysts' overall performance. We extrapolate the functions expected of a SOC analyst from what we call "*Global SOC Functions*" by identifying services offered by a SOC and mapping the activities of analysts to these functions. We report the following factors and criteria: *quality of an analyst's analysis, quality of an analyst's report, time-based measures* and *absolute numbers derived from analysts' tasks* as the main KPI relevant to obtaining the overall performance of an analyst. To the best of our knowledge, this is the first study to identify and present the main KPI for capturing analysts' performance based on several aspects of analysts' function using empirical data collected from analysts and SOC managers.

The remainder of this paper is organized as follows: Section II presents background information. Section III presents the methodology adopted for this study. In Section IV, we present our analysis and study findings. Section V presents our discussion. Section VI introduces our proposed framework, followed by Section VII which discusses related work. Section VIII concludes the paper.

II. Background

A. *The Role of the Analyst*

A SOC does not function by itself, but rather it is supported by a number of teams who work collaboratively to achieve the SOC's objectives [6]. While roles such as SOC analysts, SOC engineers, SOC manager, along with a chief information security officer (CISO), exist in most SOCs, prior works suggest that analysts are responsible for threat identification; analyzing security incidents; and recommending mitigation actions to ensure the confidentiality, integrity and availability of an organisation's information systems [8], [14].

Most SOCs generally operate a tiered team structure with specific role assignments to analysts: Tier 1 analysts (level 1 analysts); Tier 2 analysts (level 2 analysts); and Tier 3 analysts (level 3 analysts) [4]. Tier 1 analysts are oftentimes the junior analysts and the least experienced analysts [16]. Tier 1 analysts are responsible for all initial investigations, triaging of events and deal with the majority of all incidents [8]. They are also responsible for attending to most phone calls and emails directed to the SOC. Additionally, Tier 1 analysts are responsible for raising initial tickets on events that require investigation, performing initial analysis, managing the tickets until it is resolved and closed. Tier 1 analysts will escalate incidents they cannot resolve to Tier 2 analysts.

Tier 2 analysts are responsible for in-depth analysis of incidents escalated by a Tier 1 team [8]. Once they receive or identify an incident, the Tier 2 team will be responsible for its management until it is closed or escalated to Tier 3 analysts. Depending on the nature of an organisation, Tier 2 analysts may have responsibilities such as signature tuning; writing use cases and amending existing use cases; basic device configurations such as the installation of IPS, IDS, vulnerability management; configuring log and event collectors [17].

Tier 3 analysts are usually the most experienced analysts. The Tier 3 team are expected to possess and demonstrate a higher level of competences within the domain of cybersecurity. The day-to-day role of members within Tier 3 includes management of incidents escalated by Tier 2; sharing and managing threat intelligence; implementation, configuration and optimization of security tools. Tier 3 analysts may also write customized signatures; create use cases and maintain security policies on security solutions such as firewalls, intrusion detection and prevention systems; and in some cases act as consultants to SOC managers [17]. It is important to note that despite the tier structure, many of the tasks and responsibilities may overlap [4], [8]. Also, some SOCs are moving away from a tiered structure to a single analyst role and replacing many of the existing manual tasks with SOAR (Security Orchestration, Automation and Response) [18]. Besides analysts, there are also other security professionals such as SOC engineers working in a SOC, as mentioned earlier. However, the focus of this study is on analysts. As such, other roles will not be discussed in this work.

To ensure that analysts are meeting the objectives and goals of the SOC, managers draw on metrics to assess their performance. The word '*performance'* in the context of this study can be defined as how well or badly a person does a piece of work or an activity [19]. Prior works suggest that there is a tendency for studies to focus on technology whilst ignoring the vital human element, even though SOC is made up of people, processes and technology [8]. Unfortunately, one of the problems with existing assessment methods is that several factors of the tasks expected of analysts are not taken into consideration according to the literature [11], [14]. This work takes steps towards contributing to filling this gap by identifying the main function expected of the analyst, amongst a list of many services offered by the SOC.

Given that it is the analyst that makes most of the final decisions during operations [6], it comes as no surprise that their performance is of interest to stakeholders and SOC managers [14]. In fact, Shah et al. [20] explain that effective performance, such as the timely analysis of alert by the analysts is an essential characteristic of an efficient SOC. SOC managers and stakeholders, therefore, maintain a range of metrics and measures for the analysts. Next, we discuss the need for metrics and measures for a SOC analyst.

B. *The Need for Analysts' Performance Metrics and Measures*

To appreciate the terminologies used in this work, a recap of the terms "metric" and "measure" are presented below. Black et al. [21] define a metric as a subjective, latent attribute that can have several measures. A measure, on the other hand, is concrete, objective and quantifiable data that can be used to create a metric. According to Sundaramurthy et al. [14], metrics impact on analysts' perception of their performance. They state that the more reflective a metric is to the analyst's achievements, the greater their confidence when it comes to management evaluation. However, as they acknowledged, devising a useful performance metric is a challenge, as SOC managers do not even know what the right metric should be [14]. This problem is further complicated by the fact that the main functions of analysts that need to be taken into consideration when assessing analysts' performance have not been investigated by prior works, to the best of our knowledge.

While SOC managers and stakeholders rely on several qualitative and quantitative metrics and measures to assess the performance of analysts, the perception gleaned from literature is that these metrics and measures only focus on limited aspects/understanding of analysts' operations. In fact, unless the key functional areas and aspects that should be measured are identified, from our perspective, it is not likely one can obtain insight into the holistic efforts of an analyst's performance. Equally, unless holistic efforts of analysts' performance are tracked, poor performance cannot be identified for appropriate action to be taken to improve productivity [22].

Metrics and measures can be used to identify an analyst's strength and to identify analysts' training needs requirement. Unfortunately, extant literature posits that existing metrics do not fully reflect the efforts of analysts, which leads to dissatisfaction and drives down morale [14]. The question to ask is whether analysts' and SOC managers' views can be elicited to solve this current problem. This work takes steps towards answering this key question with the aim of using the knowledge gained to act as the foundation to establish how the performance of analysts can be evaluated.

III. Methodology

To design our framework, we adopted a qualitative research approach and drew on the case study research design suggested by Yin [23]. In our work, we wanted to investigate two important questions: (1) What are the main functions of a SOC analyst within a Security Operations Center? (2) What factors and criteria should be taken into consideration when assessing the performance of the analysts? To answer our research questions, we collected empirical interview data from analysts and SOC managers; we reviewed analysts' workflow models/documents; carried out observation of analysts' in a SOC and analyzed multiple sources of literature on SOCs [3]–[7], [10]–[12], [17]. Our case study design approach is similar to the work of Schinagl et al. [6], who proposed a framework for building SOC.

Given that our study is exploratory in nature, we engaged with analysts and SOC managers to solicit their views on key analysts' functions and the factors/criteria by which analysts' efforts should be measured against. Prior to engaging with participants, we sought ethical approval for our work from our institutional research ethics committee, as analysts and SOC managers are human subjects.

The initial set of participants were recruited using contacts from the SOC industry. We then adopted a snowballing approach and requested participants to recommend other analysts and SOC managers that may be interested in taking part in this study. This strategy is similar to the approach adopted by Kokulu et al. [4]. All participants were asked to sign a consent form to approve their willingness to take part in the study. Once recruited, we requested participants to take part in a 1-hour one-to-one interview to share their opinions on SOC functions, analysts' tasks, metrics and measures for analysts along with human factors that impact on their performance. To protect the participants' identity, we used aliases.

The interview questions were designed using insight from existing works and are grounded on the functions of a SOC suggested by previous researchers [5]–[7], [24]. The interviews were tape-recorded and later transcribed. Handwritten notes were taken during the interviews. During the interview, the tentative framework devised using insight from existing works was presented to the analysts to solicit their feedback. This was an opportunity for the analysts to comment on their functions and that of a SOC. The strategy of presenting a tentative framework to participants is similar to the work of Schinagl et al. [6]. To improve the credibility and the validity of our study we used multiple sources of evidence and interviewed multiple participants from different industries and applied the qualitative member check technique [25]. We did not stop conducting interviews until reaching a point of data saturation where new themes stopped emerging [26], [27].

IV. Analysis and Study Findings

Eight (8) SOC analysts and four SOC (4) managers participated in our interviews. All the interviews were conducted face-to-face. Our participants were from five different industries: defence, airline, finance (banking), a global telecom company and the automobile industry. The participants were all experienced analysts and managers in their respective organisations. *TABLE 1* shows the profile of our participants.

TABLE 1. PARTICIPANTS PROFILE AND THEIR ORGANISATIONS

Interviewee ID	Type of Industry	Job Title	Years of Experience
I1	Airline	SOC Analyst	8
I2	Airline	SOC Manager	5
I3	Defence	SOC Analyst	5
I4	Defence	Senior SOC Analyst	9
I5	Managed Security Service Provider (MSSP)- Utility and Airport	UK SOCs Manager	14
I6	Airline	SOC Analyst	5
I7	Airline	SOC Analyst	4
I8	Defence	SOC Analyst	6
I9	Defence	SOC Manager	2
I10	Finance (Banking)	SOC Consultant	7
I11	Telecom	Cyber Operations Specialist	5
I12	Automobile (Aerospace and Defence)	Cyber Incident Director and Head of Security Operations	10

The engagement with SOC analysts and SOC managers resulted in several pages of interview transcript. To organize our data, we used the software package Nvivo 12. Nvivo does not perform any analysis but acts as a useful tool for organizing our data and complements our manual coding. To carry out our analysis, we opted for an accessible and flexible technique to analyze our interview data using thematic analysis [28], [29]. According to Braun and Clarke [29], there is no ideal method for analysing interview data, however, the selected method must match what the researcher seeks to uncover. Thematic Analysis (TA) offers a useful method for identifying themes and patterns in data collected from the participants [28]. Under TA, researchers often use direct quotes and paraphrasing to increase the credibility of their analysis based on the data [28].

TA, however, is a broad approach with several sub-methods, giving a researcher an additional choice. The use of a tentative framework made one particular type of TA method the most appropriate for our work. This method is known as Template Analysis, developed by King [30]. In using Template Analysis, we draw inspiration from the work of Sundaramurthy and his colleagues on SOCs which utilizes a similar data analysis technique [31]. The template analysis process followed to analyze our data is described below.

We began our data analysis using '*a priori' theme***,** which is allowed under template analysis, unlike some other forms of thematic analysis techniques such as Braun and Clarke's version of TA [32]. The initial set of themes were developed based around the functions of a SOC, tasks expected of the analysts and metrics for assessing analysts' performance, as identified in existing works. We then proceeded to *transcribing* our audio-recorded interviews and reading through the interview transcripts to *familiarize ourselves* with the data. Sections of the interview notes relevant to the research questions were identified during the *initial coding*. We highlighted sections of the text that were relevant to understanding our objectives [32]. We applied *a priori* codes to those parts of the data. When a section of the interview data matches a research question, where there is no existing code, a new code is devised to cover it. The findings reported here are based on preliminary results of ongoing fieldwork. We continue to apply our develop template to our data set towards our effort to design a comprehensive approach for evaluating analysts' overall performance.

A. *The main functions of an analyst in a SOC*

This section addresses the research question 1. Our participants mentioned several functions of a SOC and point out key tasks expected of analysts under different functions. *TABLE 2* provides a summary of the main functions of a SOC and typical activities expected of the analysts undertaking the associated function. SOC functions identified are:

Monitoring and Detection Function – Entails monitoring of computer network systems, devices and applications running on these devices to detect malicious or abnormal activity. One of our participants, I5, who is a SOC manager with fourteen years SOC experience, stated that the monitoring and detection function is at the heart of the SOC operation as it is the means by which threats can be identified by an analyst.

Analysis Function – This function involves an in-depth investigation into observed abnormal/unusual activities seen across an organizational network. I3 stated that "you have to analyze all traffic and packets to know what is going on".

Response and Reporting Function – Involves the analyst taking specific actions as mandated by their local working processes to mitigate or reduce potential damage from an identified threat. I3, who manages an airline SOC, mentioned that response and reporting function is a primary function for an analyst. He argued that "there is no point of monitoring if you are not going to respond and report any abnormal activity". Response function also entails producing both technical and non-technical reports to relevant stakeholders on incidents.

Intelligence Function – Entails gathering of information on specific indicators of compromise (IOCs) from third parties and open sources to detect malicious activities. I10, who is a SOC consultant at one of the UK's largest banks, explained that intelligence function is a crucial component of the services offered by a SOC.

TABLE 2. GLOBAL SOC FUNCTIONS AND ANALYST TASKS

SOC FUNCTIONS	ANALYST FUNCTIONS AND ACTIVITIES
Monitoring and Detection Function	•Monitor 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.
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
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
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.
Baseline and Vulnerability Function	•Vulnerability Scans •Patching and Patch management. •Finding vulnerabilities within the environment and applying patches.
Policies and Signature Management	•Writing and Tuning Correlation Rules •Content Modification to remove false positives.
Compliance and Risk Management Function	Compliance Scans and Reporting
Incident Management/Handling Function (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned)	Partly covered by Analyst but predomintely carried out by Incident Handlers working in a Computer Security Incident and Reponse Team (CSIRT)
Pentration (Pentest) Function/Red Team	A Pentester Function
Forensic and Malware Analysis Function	A Forensic Expert Function
Engineering and Collection Function	SOC Engineer

Incident Management Function – Jacobs et al.[5] state that incident management is the ability to prepare, identify and escalate an incident. I1 and I5 highlight *incident management function* as an integral part of a SOC operation. According to I1, SOCs must have a containment and eradication plan as part of the overall incident management function.

Baseline and Vulnerability Function – This function entails patching and hardening of systems to address any known weaknesses in the system. I1 mentioned that analysts are expected to carry out vulnerability scanning of systems and report on any identified weaknesses.

Policies and Signature Management Function – The SOC needs to maintain up-to-date use cases, also known as policies, and signatures on their technical toolings such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) to detect cyberattacks. I10 states that poor use case and signature management will result in excessive amounts of false positives and increase the workload for an analyst.

Compliance and Risk Management Function – This function entails the SOC supporting the business to meet any mandatory, industrial or regulatory requirements. Additionally, a SOC can support a business to identify the risk that they face. I10 mentioned that if SOCs do not know the risk that the business faces, they cannot create effective use cases, policies or implement effective security controls.

Penetration Testing (Pentest) Function – Involves the SOC simulating cyberattacks against an organisation's computer network systems to test their current defences and how it will react when under attack. Participants mentioned that penetration testing is not a function for an analyst. For example, I10 and I11 mentioned that their SOCs employed a specialist to conduct these functions.

Forensic and Malware Function – Entails the gathering and preservation of evidence relating to malicious activities in a manner that is acceptable to a court of law. I3, I9, I10 and I12 all mentioned that forensic and malware function is an important capability of a SOC. However, participants that mentioned this function explained that activities under this function are often carried out by a specialist team. For example, I3 described that forensic and malware functions are carried out by a specialist team that works closely with law enforcement agencies.

Engineering and Log Collection Function – Maintenance of a SOC tooling and collection of logs is an essential component of a SOC. I5 stated that it would be impossible to detect attacks if a SOC did not collect logs from their network. He explained that although this is a function of a SOC, activities under the engineering and log collection would be conducted by a SOC engineer rather than an analyst. Jacobs et al. [5] state that log collection provides a centralized place for aggregating all security events and transactional activity.

B. Assessing the Performance of Analysts

This section relates to research question 2. Our participants talked about several factors that should be taken into consideration when assessing their performance, along with existing metrics and measures used in their SOCs. Over 90% of our participants argued for analysts' performance to be based on the "quality of their analysis" and the "quality of their report" rather than focusing on numbers, such as the number of tickets closed or opened. For example, I10 suggested that "rather than just the output of what analysts are doing, they should be measured on the quality of their work". A similar theme was observed across our data set. We found this surprising as most existing work typically talks about the use of absolute numbers, such as the number of incidents raised along with the mean time to detect (MTTD) and the mean time to respond (MTTR) [7], [8], [14].

Quite often participants used the terms "*metric*" and "*measure*" interchangeably. The confusion between a metric and a measure was not a surprise because even cybersecurity researchers fail to make the distinction clear and some even use them interchangeably [33]. The top metrics and measures discussed by our participants are shown in *TABLE 3*.

The quality of an analyst's analysis and quality of their report were identified as the main KPI analysts and managers preferred. While there seems to be an agreement between SOC managers and their analysts on how analysts' performance should be measured, the problem with the quality of analysis is that it is entirely subjective. I7, I8 and I11 point out that quality analysis is a reflection of the report written by the analyst as no one can know what is happening in the "*head*" of an analyst unless they document any analysis carried out in their report. Based on our analysis we argue that if "quality analysis" resides anywhere in a SOC, it will reside in the report written by the analyst.

TABLE 3. TOP METRICS AND MEASURES MENTIONED BY PARTICIPANTS

Metric	Merit	Drawback
Number of Incidents Raised	Easy to see analysts raising the majority of the incidents received by the SOC. Drive analysts to wanting to do more.	Does not take into account the severity or priority of the incidents. Does not account for analysts carrying out a detailed investigation.
Time taken to Detect, and Time taken to Respond to an Incident	Useful for assessing the vigilance of an analyst. Useful for tracking if analysts are taking too long to respond to events and incidents	Difficult to put a timeline on how quick analysts should identify an incident. Can lead to analysts spending less time to understand the root cause of the alert. Does not take into account the gathering of collaborative evidence and stealthy attacks.
Number of Incidents Closed	Easy to see proactive analysts and those raising the majority of the incidents. Useful for tracking a fair share of incident closure within the team.	Does not take into account complexity of the incidents. May be outside of the analyst control.
Quality of Analysis	The benefit of this measure is that it focuses on the quality of analysts work as opposed to quantity.	Subjective and therefore difficult to measure.
Quality of Incident Report	The benefit of this measure is that it focuses on the quality of analysts work as opposed to quantity.	Subjective and therefore difficult to measure.

V. DISCUSSION

This study focused on identifying the primary functions of a SOC and the key tasks expected of analysts within a SOC to facilitate the design of an approach to capture analysts' holistic performance. In this work, we deduce the functions of analysts from the functions and services typically offered by a SOC. We introduce the term "*Global SOC Function*" to denote the major services expected from a SOC and argue that any organisation offering SOC services will offer at least one of the services in our framework. This claim was validated and confirmed by our study participants.

Several themes emerged during our engagement with the participants. While we started with six initial themes on the functions of a SOC, five additional functions emerged during our engagement with the analysts, as shown in *TABLE 2*. Although functions such as malware and forensic analysis were reported by analysts and also reported by existing literature [6], [7], our participants acknowledged that it was not a function for analysts. One participant, I10, commented that "we also have a forensic capability….but work is done by a forensic specialist but still part of our team". Likewise I7 commented that, "I am an analyst and not a pentester but I engage with pen testers to create use cases that can feed into the intelligence function of a SOC", again, illustrating that pen-test activities are outside the remit of analysts. Analysts would not be expected for their performance to be based on forensic and pen-test functions.

We observed a number of recurring themes specifically on the functions expected of the analysts. All our participants agreed that analysts will be expected to monitor, detect, analyze and report security events. Indeed, the consensus was that these four activities: monitor, detect, analyze and report are at the core of analysts' operations. Another observation is that baseline and vulnerability management, compliance and risk management function, along with polices and signature management functions, are not always carried out by analysts.

Another interesting key pattern within our data relates to analysts' and SOC managers' agreement on the use of quality of analysis and quality of report as the assessment method. From our perspective, even though the word "quality" is subjective and difficult to measure, we are of the opinion that guidelines can be provided to assess the quality of analysis of analysts' work and of their reports. D'Amico and Whitley [13] talk about different analysis conducted by analysts. I12, who is a cyber incident director and head of security operations, states that a guideline for assessing the quality of analysis is long overdue. We happen to concur and argue that unless there is a guideline on "how to" evaluate the "quality of analysis", quality analysis will remain mysterious, potentially resulting in "elitists" among some analysts, who may see themselves as "seniors" or "experienced". We also argue that having guidelines for evaluating quality analysis will help junior/inexperienced analysts to improve their analysis. Guidelines can also be useful in addressing the issues around tacit knowledge.

When it comes to the use of time as an assessment method, analysts do not necessarily agree that managers should put a time on their activities because often times there are issues such as stealth attacks and reliance on third parties for collaborative evidence, which are outside their control. Analysts, however, recognize that SLA can mandate specific actions to be taken within certain timeframes. Although analysts and SOC managers preferred performance to be based on the quality of analysis and report, they acknowledged that using '*absolute numbers'* is easier, as assessment based on "quality" is subjective.

Based on the data received and our analysis of existing literature [5]–[7], [24], we next present core analysts functions and KPIs relevant for evaluating analysts performance.

VI. TOWARDS ANALYST FUNCTIONS AND KPI FRAMEWORK

In this section, we present factors that can be used to develop an approach for evaluating the overall performance of an analyst. While a SOC offers several services and functions, our fieldwork led us to uncover the real analysts' functions and key performance indicators (KPIs) that should be taken into consideration to assess analysts' performance. Using empirical data collected from our participants and insight from existing works [5]–[7] [24], we propose the framework in *Fig 1*, depicting SOC functions, the functions expected of analysts and the main KPIs. Our framework has several parts/components. The components contained in the bottom half of our framework in the blue dotted line represent the eleven main functions of a SOC.

Among the eleven functions identified, the functions in the red boxes are not performed by analysts but by a specialist team. The green filled boxes are the functions reported by our participants as foundational to any SOC. Participants expect any assessment method to take monitoring, detection, response and reporting into consideration. The blue boxes located in the blue dotted line: intelligence function, policies and signature management functions, baseline and vulnerability function, incident management function, along with compliance and risk management functions represent add-on functions for many SOCs, as reported by our participants.

The top section of the framework, represented by the red dotted lines, represents the basic (*primary*) functions of a SOC. The red arrow between the yellow and the pink filled boxes illustrates that 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 filled box. The criteria reported by participants as relevant to the assessment of analysts are represented in the orange filled box (quality, time and absolute number). Finally, the purple box contained in the red dotted line illustrates the main KPI participants suggest as required to capture the actual performance of analysts in a SOC.

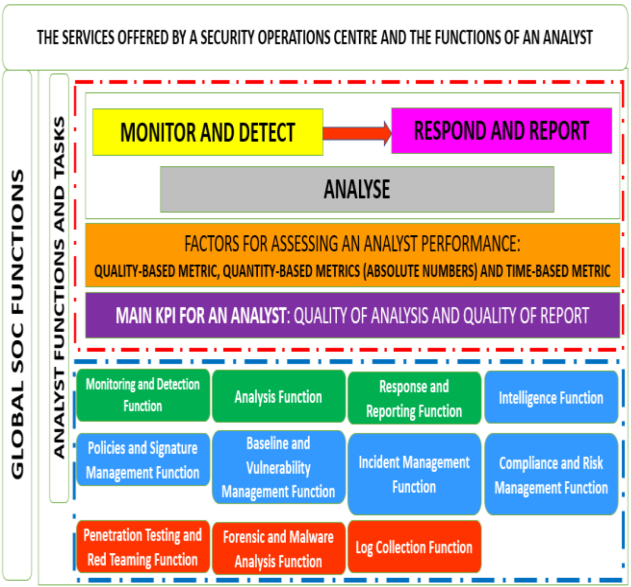
THE SERVICES OFFERED BY A SECURITY OPERATIONS CENTRE AND THE FUNCTIONS OF AN ANALYST
GLOBAL SOC FUNCTIONS
ANALYST FUNCTIONS AND TASKS
MONITOR AND DETECT
RESPOND AND REPORT
ANALYSE
FACTORS FOR ASSESSING AN ANALYST PERFORMANCE:
QUALITY-BASED METRIC, QUANTITY-BASED METRICS (ABSOLUTE NUMBERS) AND TIME-BASED METRIC
MAIN KPI FOR AN ANALYST: QUALITY OF ANALYSIS AND QUALITY OF REPORT
Monitoring and Detection Function
Analysis Function
Response and Reporting Function
Intelligence Function
Policies and Signature Management Function
Baseline and Vulnerability Management Function
Incident Management Function
Compliance and Risk Management Function
Penetration Testing and Red Teaming Function
Forensic and Malware Analysis Function
Log Collection Function

Fig 1. A framework depicting the functions of an analyst and factors that can be used to capture their overall effort.

Our framework has some features that are similar to the risk-based framework for assessing cybersecurity capabilities of organizations proposed by the National Institute of Science and Technology (NIST), specifically within the critical infrastructure sectors [34]. Even though the NIST framework contains many of the core functions of a SOC such as identify, protect, detect, respond and recover, as shown in below in *Fig 2*, the actual framework in itself is not aimed at a SOC per se, to allow the identification of the main functions of analysts, in order to evaluate their holistic efforts.

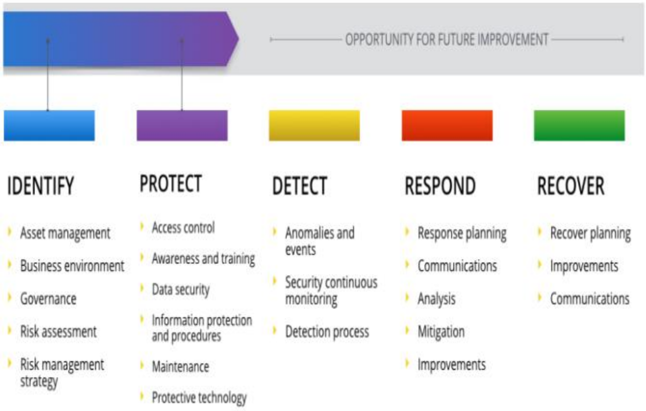

Fig 2. NIST Cybersecurity Framework [35].

Using our proposed framework, we argue that analysts' holistic effort can be captured. We aim to do this as future work. This will assist SOC analysts, managers and stakeholders to assess analysts' performance across the various functional areas. Cybersecurity researchers can also rely on our framework to develop new sets of performance metrics for the various functional areas.

VII. Related Work

There have been prior works that seek to understand the functions of a SOC and the role of the analysts in the SOC. D'Amico and Whitley [13] investigate and report on how computer network defence (CND) analysts conduct analysis and report on six types of analysis often performed by analysts. They conclude that visualizations could support data analysis and facilitate the work of CND analysts.

An anthropological study conducted by Sundaramurthy et al. [8] at three different SOCs identified team structures in a SOC, operational workflows of a SOC, along with several metrics for assessing analysts' performance. Metrics reported in their work are the number of incidents raised by analysts, the use of success stories and the time it takes analysts to create a ticket. However, they acknowledge that existing metrics are inadequate and advocate for research to devise useful metrics for analysts.

A continuation study by Sundaramurthy et al. [14], again using anthropology reports on burnout phenomenon among analysts as they carry out their function in the SOC. They identified factors that lead to burnout in the SOC and report on several metrics for assessing analysts' performance. They observed that analysts are dissatisfied with existing metrics as they fail to take into consideration several aspects of the tasks they perform in a SOC. Lif and Sommestad [24] proposed a model for evaluating the performance of IDS operators, however, as they acknowledge, the work of IDS operators is a subset of those expected of the analysts.

Jacobs et al. [5] proposed a model and a classification scheme for evaluating the effectiveness and capabilities of a SOC based on three aspects of a SOC: the maturity level; the SOC services; and capabilities of the services provided by the SOC. Their work identified functions of a SOC as: log collection; log retention and archival; log analysis; monitoring; threat identification and reporting. However, what they did not do was to identify which of those functions are actually performed by analysts.

Schinagl et al. [6] present what they called a generic building block of a SOC and identify several functions of a SOC. Using these functions, they devised an assessment method to assess the effectiveness of the services provided by a SOC. Although their framework has been accepted by the Dutch security community as a model for building SOCs or improving SOC services, the authors did not elaborate on specific analysts' tasks or functions expected of analysts that should be measured to capture their holistic performance.

Onwubiko [7] presents a framework for a SOC that consists of log collection, analysis, incident response, reporting and continuous monitoring. He briefly discusses a number of metrics for assessing the performance of analysts, which are consistent with metrics suggested by Sundaramurthy and his colleagues [8], [14].

Kokulu et al. [4] conduct a qualitative study on SOCs to identify the main issues and challenges faced by SOCs. Among the numerous issues reported was ineffective metrics in SOCs. They argued that current quantitative metrics such as the number of incidents raised and time taken to react to an incident are not effective, because they fail to take into consideration the severity and priority of the events.

The main difference between this work and that of previous work is that we identify the key analysts' functions and factors that need to be taken into consideration to evaluate the holistic effort of analysts. None of the studies described in the related work identifies criteria that need to be taken into account to capture the holistic performance of an analyst.

VIII. Conclusion, limitation and future work

SOC analysts are expected to demonstrate high human performance, as poor performance impacts on the efficiency of a SOC. To evaluate the performance of analysts, SOC managers and stakeholders use metrics and measures. However, existing literature points out that extant metrics and measures are unsatisfactory as these fail to take into consideration the several functions of a SOC analyst. Currently, there is no agreement on what constitutes the core functions of analysts. Using empirical data and insight from prior works, we propose a framework that captures the main functions expected of the analysts and factors that need to be taken into consideration to assess the efforts of analysts. To the best of our knowledge, this is the first empirical study to provide core factors that can be used to develop a holistic approach to evaluate analysts' performance.

Our research results indicate that SOC functions that should be taken into consideration when assessing analysts performance are: monitoring and detection function;

analysis function; response and reporting function; intelligence function; baseline and vulnerability function; along with policies and signature management functions. Among these functions, analysts and SOC managers identify monitoring and detection, response and reporting, along with analysis function as foundational and advocate for these to be included in any performance assessment. The following factors/criteria: *quality of an analyst's analysis*, *quality of an analyst's report*, *time-based measures* and *absolute numbers derived from analysts' tasks* were identified as the main key performance indicators necessary for evaluating the performance of the analyst.

A limitation of this work is that although the member-checking strategy used in this study is considered as one of the validation techniques of qualitative research, it remains subjective and limited to the opinions of the participants. Future work will focus on extending our framework to propose a new approach for measuring analysts' performance.

Acknowledgment

We appreciate the efforts of all the participants for their cooperation. Without their insight, this work would not have been possible.

References

[1] Department of Health and Social Care, "Security cyber resilience in health and care," London, 2018.

[2] 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)*, 2017, pp. 173–175.

[3] N. Miloslavskaya, "Information security management in SOCs and SICs," *J. Intell. Fuzzy Syst.*, vol. 35, no. 3, pp. 2637–2647, 2018.

[4] F. B. Kokulu, T. Bao, A. Doupé, Y. Shoshitaishvili, G.-J. Ahn, and Z. Zhao, "Matched and Mismatched SOCs : A Qualitative Study on Security Operations Center Issues," *Assoc. Comput. Mach.*, 2019.

[5] P. Jacobs, A. Arnab, and B. Irwin, "Classification of Security Operation Centers," in *2013 Information Security for South Africa*, 2013, pp. 1–7.

[6] 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*, 2015, vol. 2015-March, pp. 2253–2262.

[7] 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)*, 2015, pp. 1–10.

[8] 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*, 2014, pp. 43–50.

[9] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *J. Inf. Secur. Appl.*, vol. 48, p. 102352, Oct. 2019.

[10] 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 Comput.*, vol. 21, no. 3, pp. 40–46, May 2017.

[11] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Challenges and performance metrics for security operations center analysts: a systematic review," *J. Cyber Secur. Technol.*, pp. 1–28, Dec. 2019.

[12] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, 2014.

[13] 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*, 2008, pp. 19–37.

[14] Sundaramurthy *et al.*, "A Human Capital Model for Mitigating Security Analyst Burnout," in *Symposium on Usable Privacy and Security*, 2015, pp. 347–359.

[15] E. Dafikpaku, "The Strategic Implication of Enterprise Risk Management (ERM): A Framework," in *ERM Symposium*, 2011, vol. 48.

[16] P. B. Hámornik and C. Krasznay, "A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers," 2017, pp. 224–236.

[17] A. E. Thomas, *Security operations center : analyst guide*. London: CreateSpace, 2016.

[18] P. Mcevatt, "Advanced Threat Centre and Future of Security Monitoring," *FUJITSU Sci. Tech. J.*, vol. 55, no. 5, pp. 16–22, 2019.

[19] Oxford Dictionaries, *Oxford Dictionary of English.*, 3rd Ed. Oxford: Oxford University Press, 2010.

[20] A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "Understanding Trade-offs Between Throughput, Quality, and Cost of Alert Analysis in a CSOC," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1155–1170, 2018.

[21] J. G. Voeller, P. E. Black, K. Scarfone, and M. Souppaya, "Cyber Security Metrics and Measures," 2008.

[22] K. Siregar and S. F. Siregar, "Design of mathematical models assessment of working achievements based on spencer competency in PT. Z," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 309, no. 1, 2018.

[23] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. Los Angeles: Sage Publication, Inc., 2018.

[24] P. Lif and T. Sommestad, "Human factors related to the performance of intrusion detection operators," in *HAISA*, 2015, pp. 265–275.

[25] D. R. Thomas, "Feedback from research participants: are member checks useful in qualitative research?," *Qual. Res. Psychol.*, vol. 14, no. 1, pp. 23–41, Jan. 2017.

[26] P. I. Fusch and L. R. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *Qual. Rep.*, vol. 20, no. 9, pp. 1408–1416, 2015.

[27] E. Costa, A. L. Soares, and J. Pinho De 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*, 2016, pp. 531–544.

[28] J. Aronson, "The Qualitative Report A Pragmatic View of Thematic Analysis," *Qual. Rep.*, vol. 2, no. 1, pp. 1–3, 1995.

[29] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006.

[30] N. King, "Qualitative Organizational Research: Core Methods and Current Challenges - Google Books," in *Qualitative Organizational Research: Core Methods and Current Challenges*, London, UK: Sage publications Ltd, 2012, pp. 426–50.

[31] S. C. Sundaramurthy *et al.*, "Turning Contradictions into Innovations or : How We Learned to Stop Whining and Improve Security Operations This paper is included in the Proceedings of the Turning Contradictions into Innovations or : How We Learned to Stop Whining and Improve," in *the Symposium On Usable Privacy and Security (SOUPS)*, no. Soups, USA: USENIX, 2016, pp. 237–251.

[32] J. Brooks, S. Mccluskey, E. Turley, and N. King, "The Utility of Template Analysis in Qualitative Psychology Research," *Qual. Res. Psychol.*, vol. 12, pp. 202–222, 2015.

[33] R. K. A. Ahmed, "Overview of Security Metrics," *Softw. Eng.*, vol. 4, no. 4, pp. 59–64, 2016.

[34] M. P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," *Natl. Inst. Sci. Technol.*, 2018.

[35] A. Chang-Gu, "NIST Cybersecurity Framework vs. NIST Special Publication 800-53," *Security Blog*, 2015. [Online]. Available: https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53?edition=2019. [Accessed: 22-Dec-2019].