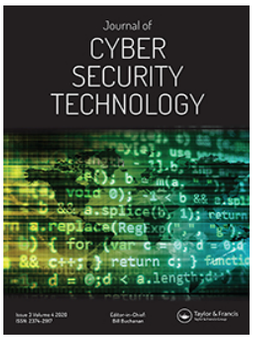

Journal of Cyber Security Technology

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tsec20

Challenges and performance metrics for security operations center analysts: a systematic review

Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke & Pete Burnap

To cite this article: Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke & Pete Burnap (2020) Challenges and performance metrics for security operations center analysts: a systematic review, Journal of Cyber Security Technology, 4:3, 125-152, DOI: 10.1080/23742917.2019.1698178

To link to this article: https://doi.org/10.1080/23742917.2019.1698178

JOURNAL OF CYBER SECURITY TECHNOLOGY
2020, VOL. 4, NO. 3, 125–152
https://doi.org/10.1080/23742917.2019.1698178

Taylor & Francis
Taylor & Francis Group

Challenges and performance metrics for security operations center analysts: a systematic review

Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke and Pete Burnap

School of Computer Science and Informatics, Cardiff University, Cardiff, UK

ABSTRACT

The increasing use of Security Operations Centers (SOCs) by organisations as a part of their cyber security strategy has led to several studies aiming to understand and improve SOC operations. However, to the best of our knowledge, there is no systematic literature review on the challenges faced by SOC analysts or on metrics for measuring analysts performance. To this end, we conducted a Systematic Literature Review (SLR) in accordance with the guidelines for undertaking SLR and analyzed papers published on SOCs between 2008 and 2018. We provide a comprehensive overview of the challenges faced by SOC analysts and of the metrics suggested in the literature for measuring analysts performance. In addition, we present a mapping between the challenges and existing performance metrics showing how the effectiveness of an analyst in addressing a particular challenge could be measured. We also discuss the drawbacks of the existing metrics and suggest directions for improvement. Our findings will enable SOC analysts and managers, as well as the academic community to gain a better understanding of the challenges impeding the performance of SOC analysts, and how analysts performance could be measured and improved.

ARTICLE HISTORY
Received 9 October 2019
Accepted 24 November 2019

KEYWORDS
Security operations center; cyber security; security analysts; performance metrics; systematic literature review

Introduction

Security Operations Centers (SOCs) continue to attract the attention of many researchers due to its role in supporting the cybersecurity strategy of many organisations. A SOC can be defined as a centralized location inside or out of an organisation comprising of people, processes and technology with the sole purpose of helping businesses to maintain cyber situational awareness, address compliance issue and threat management [1]. Businesses are embracing the services offered by SOCs in the hope of fighting off attacks and organisations that cannot afford to own a SOC rely on third-party service providers or a Managed Security Service Provider (MSSP) to provide SOC services [2]. SOCs are being deployed by government agencies, universities, commercial and private organisations to defend their network [3]. However, it is safe to say that many of

CONTACT Enoch Agyepong agyeponge@cardiff.ac.uk School of Computer Science and Informatics, Cardiff University, 5 The Parade, Roath, Cardiff, UK

the existing studies to SOC focus on technology, with little attention on human factors, SOC processes and the challenges faced by the analysts working in the SOC [4]. Extant literature on SOCs also suggests a lack of adequate measures and metrics for assessing the performance of the analysts [5].

This review seeks to investigate, synthesize and present empirical findings on the metrics and measures for assessing analysts' performance. Additionally, we report on the challenges faced by the analysts that impact on their performance in the SOC. We believe a better understanding of the challenges faced by the analyst will provide a useful insight that SOC managers and stakeholders can use to devise intervention strategies that can improve the performance of analysts. Such understanding may also be of interest to system designers and ergonomist who typically take into consideration multiple human and environmental factors during system design. Furthermore, consolidating and presenting existing measures and metrics for evaluating analysts performance will allow researchers to identify how existing metrics and measures can be improved to capture the overall efforts of analysts in a SOC.

The remainder of this paper is structured as follows: Section 2 of this paper provides an overview of the components of a SOC, relevant concepts and key definition and along with related work. Section 3 describes in detail the systematic review process, followed by Section 4, which presents the results and findings. Section 5 presents the discussion and limitations of this study, and finally, Section 6 presents the conclusion and future work.

Background

Previous studies on SOCs suggest that people, processes and technology are at the center of a SOC and that the success of a SOC is dependent on these three elements [6]. Setting up or operating a SOC is an expensive venture and businesses continually evaluate their return on security investment and how to improve overall performance [5]. Unfortunately, when it comes to assessing the performance of SOCs, the industry generally rely on statistical data generated from deployed technological solutions such as firewalls, Intrusion Detection Systems (IDSs') and vulnerability scanners to determine or assess efficiencies [7]. The problem with this approach is that it fails to take into consideration human factors (the human security analysts or people). People (SOC analysts) are key to maintaining deployed security controls, the investigation of threats and incident management of all suspicious activities [8]. Additionally, SOCs rely on a human to outsmart a malicious attacker [1]. It is the SOC analyst that decides what is suspicious and what is not, and their performance determines what happens when cyber-criminals strike [1]. It is therefore vital to understand the challenges that analysts face and its impacts on their performance in a SOC. In addition, it is essential to understand how the

performance of SOC analysts can be measured, as anything that is not measured cannot be improved [9].

McClain et al. [10], stress that analysts performance is a pertinent issue in cybersecurity as they play a crucial role in operating and maintaining the tools used by businesses to detect and respond to cyber threats. Analysts are expected to monitor, detect, analyze and report cyber threat [6]. Also, analysts are supposed to have a greater cyber situational awareness and the necessary skills to detect attacks [4]. These responsibilities and tasks make it essential for analysts to maintain a high standard of operational effectiveness and performance as a poor operational performance will hinder the overall efficiency of a SOC [7]. One would expect analysts to receive various forms of support and ongoing training to realize their objectives in the SOC.

However, defending against cyber-attacks is not a trivial task and analysts face numerous challenges, many of which affect their performance. For example, [8] point out the complexity and intensity of the work of analysts. Similarly, the volume of alerts/security events presented to the analysts, along with the multi-faceted nature of cyber attacks all presents an enormous challenge to the analysts [4,11]. There are also issues and challenges arising from human factors such as stress level of the analysts, vigilance, mental workload, fatigue along with organisational processes and technological factors that impact on analysts performance [4,12]. While these may just be instances of what may well be part of a bigger problem, and in some cases leading to analysts burnout [7, 13, 14], it remains unclear whether researchers and practitioners have a comprehensive insight into challenges faced by analysts from human, organisational and technological perspective.

Effort to understand the challenges faced by analysts are scattered across literature, disjointed and often do not provide a comprehensive view of the issue. Hámornik and Krasznay [15], state that SOCs face internal and external issues. According to Lif and Sommestad [4], extant literature contains a few pieces of information on the challenges faced by analysts. Different authors mention different problems faced by analysts. For example, Sundaramurthy et al. [7], report alert fatigue and workload as a factor that leads to analyst burnout but acknowledges that their model does not provide exhaustive coverage of multiple challenges faced by analysts. Other researchers such as Lif and Sommestad [4], identified human factors such as multitasking, situation awareness, automation, mental workload and utilises Wickens' model of information processing to show the interplay between these factors. There are also concerns about tacit knowledge and skills shortage within the industry. A comprehensive list and analysis of these challenges can be used as the basis to improve and adapt SOC services.

When it comes to assessing the performance of analysts, the literature reports a lack of adequate measures and metrics [5,7,16]. In fact, Sundaramurthy and his colleagues highlight the need to improve existing metrics for analysts [5]. In this review, we treat the terms metrics and measures differently and adopt the

definitions offered by NIST [17]. We define a measure as a concrete, quantifiable and objective attribute such as the number of incidents raised by analysts and a metric as an abstract, somewhat subjective attribute that can have many measures, for example, monitoring function metrics. In other words, measures support metrics [18]. The word performance in this context, as defined by the Oxford English Dictionary, refers to the action or process of performing a task or function.

Even though researchers have proposed various metrics for assessing the effectiveness and efficiency of a SOC, these assessment methods do not always take analysts effort and performance into consideration. For example, Jacobs et al. [2], presents a metric for evaluating the performance of a SOC based on the capability services provided and maturity levels, but do not discuss assessment method (measures or metrics) for the analysts performance. Similarly, Schinagl, Schoon and Paans [1], also propose a performance metric for SOCs, but their work does not adequately present a formal quantitative method for measuring the efforts of analysts. Some scholars, however, have identified a number of ways by which analysts efforts can be evaluated. These writers, however, often do not differentiate between metrics and measures. In most cases, the terms measures and metrics are blurred and used interchangeably by the writers [5–7]. For example, some authors suggest the number of incidents raised or closed per day as a metric for the analysts [6]. Others focus on the time taken by an analyst to detect an incident [5,7]. Based on our definition, these are measures rather than metrics. Moreover, analysts tasks are not limited to incidents raised or closed. The evidence from the literature also suggests that analysts are not satisfied with this kind of measures as it does not take into consideration several aspects of their work [7]. A much more worrying concern that literature posits is that SOC Managers also lament about the lack of good metrics for assessing analysts [7].

Despite the important role played by analysts, research continues to focus exclusively on building blocks for SOC, SOC framework and SOC technologies [1]. In fact, the literature is replete with research on the various aspects of SOC operations but not much on holistic approaches to measuring the efforts of analysts. It is with this premise that this study aims to identify the challenges faced by analysts and metrics for assessing the performance of analysts as they address these challenges. To date, there is no single study that presents a detailed overview of the state of the art on the challenges faced by analysts or how analysts' performance is measured as they address/respond to the challenges they face. The present lack of such review makes this paper an important and a timely one.

Our contribution is to gather, analyze and synthesize existing knowledge and provide an overview of all that is known about challenges faced by SOC analysts, and metrics for measuring the performance of a SOC analyst addressing the challenges they face. Additionally, we also map challenges faced by analysts with existing performance metrics. We hope that our findings will be useful to

SOC experts, the academic community and lead to a greater understanding of the challenges impeding on the performance of SOC analysts and how analyst performance is measured.

Review process

As the SOC industry matures, studies, findings and reports on SOCs has also increased, hence there is a need to provide an overview of a SOC in the context of our research. To do this, we carried out a Systematic Literature Review (SLR). A Systematic Literature Review provides a methodological process of gathering all available or the majority of literature on a topic and analyzing them to address a specific question/s [19]. The SLR process allows evidence to be gathered to provide informative and evidence-based answers to research questions [20].

Three main research questions were defined to guide the systematic review process:

- Research Question 1 (RQ1): What are the main challenges facing SOC analysts?
- Research Question 2 (RQ2): What metrics exist to measure the performance of a SOC analyst?
- Research Question 3 (RQ3): What is the mapping between the challenges faced by analysts and existing analyst performance metrics? In other words, we would like to know whether there is a metric(s) for assessing the analyst performance as he/she addresses the challenging aspects of their work identified in RQ1.

The literature search was focused on publications that investigate metrics for SOCs, the SOC analyst and analysts' challenges. Our search strategy was devised in collaboration with a subject specialist librarian and selected papers from top scientific databases such as Scopus, Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library, Association of Computing Machinery (ACM) Digital Library, and ScienceDirect. These databases were selected because they cover the major conferences and journals, and are amongst the top databases for Computer Science research [21,22]. In addition, we also searched Google Scholar and Google search engine to increase the breadth of our search. Keywords used are security operations center; cyber security; cyber operations; security analysts; performance metrics; systematic literature review. The Google search engine was used to search for grey literature and non-academic papers. Papers are selected according to the inclusion and exclusion criteria defined below.

Our protocol follows the guideline and procedures used for systematic review described by Kitchenham and Charters [19], Kitchenham and Brereton [23], along with suggestions from Silva and Neiva [21]. The protocol specified the research questions, the search strings derived from the research questions and by breaking

the research questions into ***P***opulation, the phenomenon of ***I***nterests and ***Co***ntext (PICo) [24]. Cherry and Dickson [24], highlight that using PICo provides an effective strategy to devising the inclusion criteria. In our study, we described our PICo as: **P**opulation – the SOC analysts; the phenomenon of **I**nterests as the challenges faced by analysts and metrics for measuring analysts' performance; and **Co**ntext as the Security Operations centre as shown in Table 1. The protocol also specifies the inclusion and exclusion criteria of all identified materials, quality assessment criteria, data extraction and how the data is synthesised [25].

Inclusion and exclusion criteria

The three-phase approach for selecting papers as part of the SLR suggested by Silva and Neiva [21],was adopted in this work, as it offers a straightforward approach when considering whether to include/exclude relevant papers. The three phases comprise of initial screening of papers based on the title and abstract, analysis of the papers based on the introduction and conclusion, and complete reading and quality checklist. In addition, the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) was also followed to improve the set of items selected and reported in this systematic review [26]. Our paper selection process is shown in Figure 1.

First stage: the initial screening

The first stage in our paper selection process was the extraction of papers and articles from various databases and Google search engine using keywords derived from the research questions and PICo [27]. Only papers written in English were assessed and considered. We felt that translating papers written in other languages into English can result in losing the true meaning as intended by the original author. Articles were considered if it had pertinent information relating to SOC and meet the following criteria:

- Papers that have been published in peer-reviewed journals or conference proceedings. These papers were of interest because in most cases their content has been independently evaluated for their scientific quality by subject matter experts, although some scholars point out that this may not always be true [28,29].

Table 1. PICO table.

Review Questions	What are the challenges facing a SOC Analyst? (RQ1)	What metrics exist to allow us to measure the performance of analyst addressing some of the challenging aspects of their work? (RQ2)	What is the mapping between the challenges faced by analysts and existing analyst performance metrics? (RQ3)
P	Security Analysts	Security Analyst and SOC Managers	Security Analysts
I	Challenges faced by SOC Analysts	Metrics for measuring analysts' performance	The mapping between challenges and metrics
Co	Security Operations Centre	Security Operations Centre	Security Operations Centre

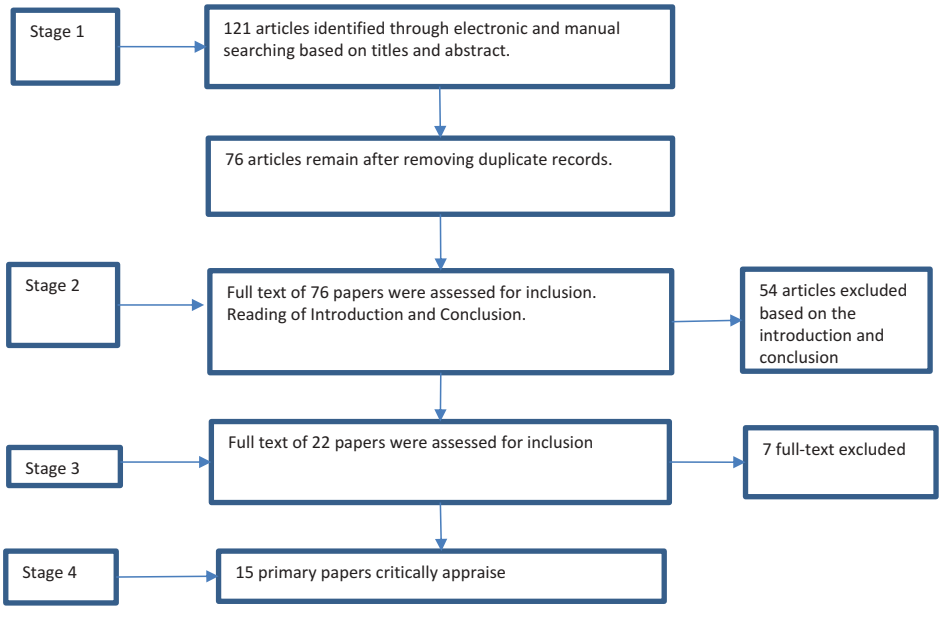

Figure 1. Paper section process.

- Articles and grey papers from a reputable organisation well-known within the cyber industry such as SANS Institute as their contents are also reviewed by Subject Matter Experts (SME) before their publications.
- Date of publication – We decided to limit our search to papers published within the last ten years allowing for a decade long analysis and comparison. However, the ten years limit does not apply to articles observed to have been cited frequently by other researchers as they could make a valuable contribution. The citation frequency of an article was therefore used as a selection criterion, although we acknowledged that a highly cited article might not necessarily be an important paper [20, p. 23]. All other studies were excluded if they are published before 2008. The references and citations of the selected papers are also traced for additional information through a snowballing process [23].

The title and abstract of each selected paper were read to establish whether it had information pertinent to the research questions and the PICo. On reading the abstract, a decision was then made whether or not a paper should be considered for the *second phase* which involves the reading of the *introduction* and the *conclusion* [21].

Second stage: reading the introduction and conclusion of each paper

The introduction and conclusion of papers that passed the first phase criteria were read to establish its relevance to the research questions further. This step is

crucial as it allowed us to eliminate papers whose abstract does not reflect their content. Papers are selected for inclusion if it addresses or contains information on the operations of a security operations centre (SOC), the functions of SOCs, challenges and problems faced by SOCs, framework/model for building SOC, operational performance of analysts, human factors in SOC, performance metrics for SOCs and SOC analysts. All other papers were excluded.

Third stage: read the entire article and undertake quality check

The final stage of the paper selection process entailed reading the full-text of all remaining papers to confirm and establish its suitability for inclusion. Studies without full-text (abstract only papers) were excluded as we believe an abstract will not provide sufficient information required for this work. We then applied a quality assessments criterion to all the papers included in our final list. Our quality assessment approach is detailed below.

Our quality assessment process focuses on the methodology used by the selected papers and is based on checklist/instrument presented by Critical Appraisal Skills Programme (CASP) [30] and suggestions provided by Dybå and Dingsøyr in [25]. Although there is no standardised quality assessment tool, Dybå and Dingsøyr along with CASP provide some vital quality assessment checklist which has been used by various researchers conducting systematic reviews in several fields [27]. Our checklist, which is adapted from the work of Dybå and Dingsøyr [25], is made up of 12 items as shown in Table 2. However, only one criterion was used as the basis for including or excluding a paper. This approach is similar to the strategy used by Dybå and Dingsøyr [25]. Notwithstanding, some scholars argue that a checklist cannot be used to assess quality [20]. However, from our perspective, using a single criterion allowed us to access a sufficient number of literature until saturation points where an additional study will not provide any new information [31].

We initially assessed the quality of each paper by answering the questions from the checklist and assigning scores based on a three-point scale of Yes (Y) = 1, No or Not Reported (N) = 0 and Partially (P) = 0.5 to calculate each paper's quality index. Given that there are 12 items on our Quality Assessment Checklist (QAC) shown in Table 3, each paper could obtain a score between 0 and 12. We used the first quartile (12points/4 = 3points) as a cut-off point for included studies. While some researchers favour this approach when assessing the quality of a paper in a systematic review [27,32] we decided to drop this technique as SOCs are still evolving and relatively new in comparison to other fields; hence applying a stringent check could result in some papers that may make valuable contribution scoring below the 3 point cut-off. We therefore decided to follow the suggestions offered by Dybå and Dingsøyr [25], described earlier.

Appendix A (Table A1) shows the data extraction forms. The information collected on each paper includes the author/s names, date of publication, method of investigation and data collection method. In addition, the form contained fields to

Table 2. Quality assessment adapted from [21,25,27].

	QC*	Quality Criteria – Question	Y/N/P
1	QC1	Is the paper based on research (or is it a discussion paper from experts)?	**Y/N/P**
2	QC2	Are the research aims specified?	**Y/N/P**
3	QC3	What research method was used: anthropology, case study, lessons learnt, opinion survey? This is based on our reading of the paper, not the method claimed by the author.	**Y/N/P**
4	QC4	Is the research method appropriate to address the aims of the research?	**Y/N/P**
5	QC5	Is there enough description of the context in which the study was conducted?	**Y/N/P**
6	QC6	Was the recruitment strategy appropriate to the aims of the research?	**Y/N/P**
7	QC7	For empirical study (apart from lessons learnt) was there a control group with which to compare treatments?	**Y/N/P**
8	QC8	Was the data collected in a way that addressed the research issues?	**Y/N/P**
9	QC9	Was the data analysis technique rigorous?	**Y/N/P**
10	QC10	Was the relationship between the researcher and participants considered to an adequate degree?	**Y/N/P**
11	QC11	Are the findings clearly laid out?	**Y/N/P**
12	QC12	Is the study of value for research or practice?	**Y/N/P**

*QC denotes Quality check

Table 3. Quality assessment outcome.

Paper	QC1	QC2	QC3	QC4	QC5	QC6	QC7	QC8	QC9	QC10	QC11	QC12
[P1) [5]	1	1	1	1	1	1	0	1	1	1	1	1
[P2] [7]	1	1	1	1	1	1	0	1	1	1	1	1
[P3] [10]	1	1	1	1	1	1	0	1	1	1	1	1
[P4] [1]	1	1	1	1	0.5	1	0	0.5	1	1	1	1
[P5] [6]	1	1	0	0	0	0	0	0	0	0	1	1
[P6] [3]	1	1	1	1	1	1	0	1	1	1	1	1
[P7] [43]	1	1	1	1	1	1	0	1	1	1	1	1
[P8] [52]	1	1	1	1	0.5	0	0	1	1	0	1	1
[P9] [12]	1	1	1	1	1	1	0	1	1	1	1	1
[P10] [38]	1	1	1	1	1	1	0	1	1	1	1	1
[P11] [39]	1	1	1	1	0.5	0	0	1	1	1	1	1
[P12] [39]	1	1	1	1	1	0	0	1	1	0	1	1
(P13] [44]	1	1	1	1	1	1	0.5	1	1	0	1	1
[P14) [39]	1	1	1	1	1	0	0	1	1	0	1	1
(P15] [15]	1	1	1	1	0.5	1	0	1	1	1	1	1

*For each paper we assigned a unique identifier (P1-P15)

collect answers to the research questions. This approach is consistent with the suggestions provided by Silva and Neiva [21]. An assumption made during the data extraction was that challenges faced by a SOC would impact on the analysts. We, therefore, treated these as challenges faced by the analysts.

The different methodologies used by the researchers of the selected papers and ways' in which the studies reported findings, made narrative synthesis the most appropriate approach for presenting the answers found to our research questions. We, therefore, carried out narrative synthesis using the information gathered from the papers. Narrative synthesis is defined as any write up of results using only word [33]. Narrative synthesis allows for the aggregation of key concepts and themes relating to the research questions identified in each of the selected papers [33].

Study findings

Our study sought to identify the challenges faced by SOC analysts and metrics for measuring the performance of analysts as they address these challenges. Over 2276 papers were identified in our keyword searches. During our searches, we decided not to use the word 'SOC' as one of the keywords because when piloted, it returned several papers, yet the majority were not relevant to security operations centres. We made an assumption that researchers writing about security operations centre will explain the acronym 'SOC' before using it; hence our chosen keywords will suffice.

Among papers returned by the databases (SCOPUS, IEEE Xplore Digital Library, ACM Digital Library, ScienceDirect, Google Scholar and Google), 121 were selected based on the title and abstract. Of these, duplicates were removed, leaving 75 papers. Only papers that explicitly mention the challenges faced by a SOC, analysts or metrics for SOC analysts were included. Fifteen papers met these criteria and were selected. Although all 15 selected papers talk about the challenges faced by analysts, only four papers report findings based on fieldwork undertaken using an ethnographic method, anthropology and case study. Likewise, only five studies reporting performance metrics for the analyst devised an approach to measure analysts' performance. Figure 2 below shows the number of publications on SOCs since 1980 taking from the key computer science databases. As shown in Figure 2, very little research was conducted on SOC in the early 1980s. The low level of research during this period can be attributed to the fact that SOCs only emerged around the late 1970s according to a business white-paper by Hewlett-Packard (HP) [34]. The majority of research on SOCs began in the early 2000s as seen in Figure 2. This observation confirms previous remark made by Miloslakaya [35], that most studies on SOC deserving attention were published

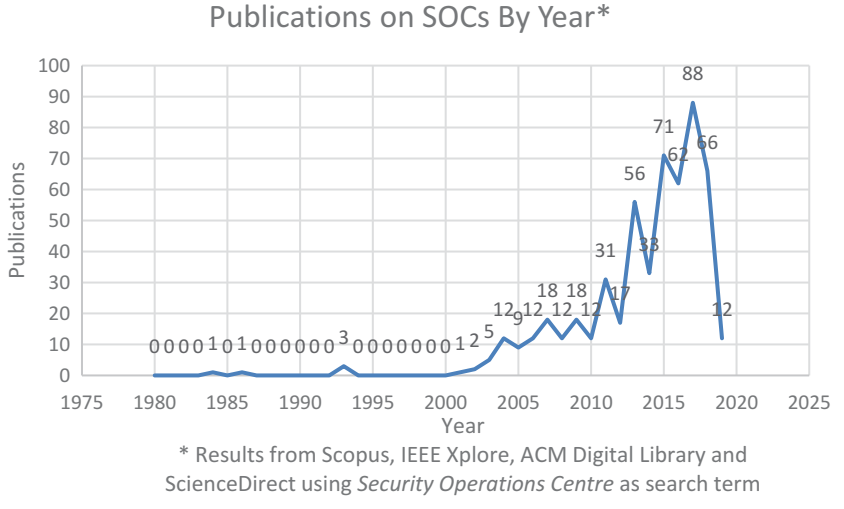

Figure 2. Publications on SOCs since 1980.

in the late 1990s to early 2000s. We noted that papers published before 2008 did not discuss issues on metrics for the analyst or the challenges they face. Also, the sharp drop in publication to 12 articles is due to the fact that the final search of publication on SOC was carried out in the middle of February 2019.

Appendix A (Table A1) presents a summary of all articles included after applying the inclusion and exclusion criteria. Key themes addressing the research questions were extracted and presented in the next section, narratively.

Challenges faced by analysts

Papers reporting challenges faced by analysts based on research are limited, and often the writers/researchers do not adequately address how these challenges can be reduced or mitigated from the native (analyst) perspective. Lif and Sommestad [4], highlight how existing literature has little information on challenges faced by analysts. Figure 3 shows the distribution of the challenges facing analysts identified in the selected papers along with the percentage breakdown of the various challenges as identified in the literature. The selected papers identified the following themes as the challenges faced by SOC analysts:

- **The Volume of Alerts** – An alert is also known as event and refer to any observable occurrence generated by a computer system [36]. Several authors report the number of alerts presented to the analyst as one of

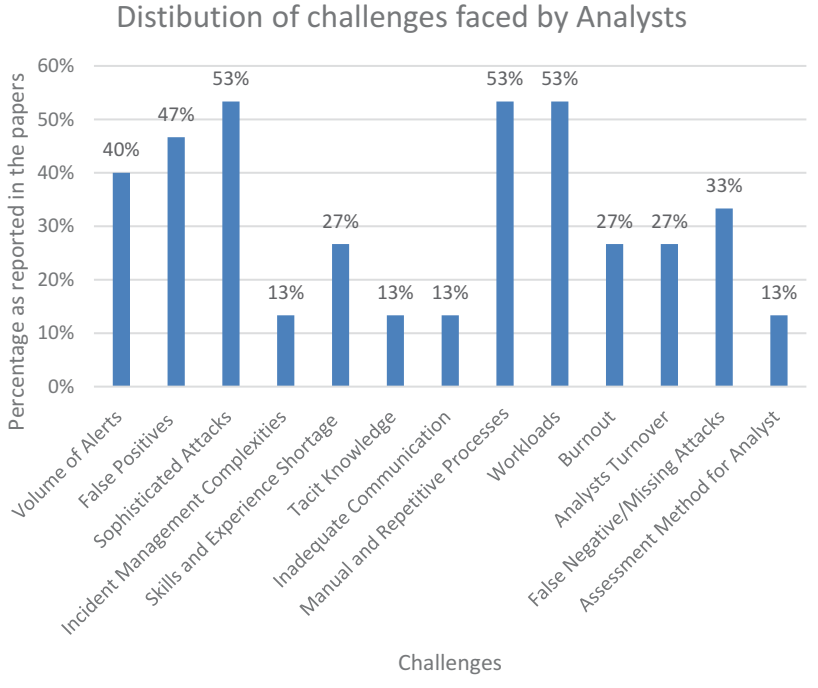

Figure 3. Distribution of challenges faced by analysts as reported by the literature.

the main challenges faced by analysts (P5, P6, P10, P12, P13, P14). A large volume of alerts means analysts often struggle to find true attacks among the mist of many alerts. Onwubiko [6], points out that not all alerts lead to an incident as there are false incidents (false positives). Incidents are events or alerts that pose a threat [36]. Limiting log collection to important assets/devices, policy tuning and filtering out unnecessary alerts (noise) have been suggested by some writers/researchers as some of the techniques that can be used to address these challenges [6]. Despite these recommendations, the evidence from the literature suggests that analysts continue to struggle when it comes to the volume of alerts they process [37].

- **False Positives (FPs)** – FPs are reported by several authors as one of the many challenges' analysts have to deal with (P1, P5, P6, P8, P10, P11 and P13). FP represents the number of 'false alarms' presented to the analysts [3, 44]. These alarms are not true attacks (true positives) but are falsely presented to the analyst as though they are, causing them to initiate some form of investigation thereby wasting analyst time. 47% of the selected papers discuss the challenge posed by FPs and highlight that FPs contribute to the high number of alerts presented to the analysts. Like the volume of alerts, FP's are also the result of collecting too many logs. Lif and Sommestad [4], warn that too many FPs can result in an IDS operator completely ignoring alerts. Factors such as misconfiguration of systems and weak signature/detection strings designed by the vendor or the analysts that incorrectly matches legitimate network traffic. Recommendation for reducing FP include tuning policies and machine learning [38]. Businesses can also put in more efforts into addressing misconfiguration issues to reduce the burden on analysts. Tuning of policies and excluding false positive forms part of the work of an analyst [6].
- **False Negatives (FNs)** – FNs are also reported by 33% of the selected papers. P6, P8, P10, P11 and P13 all identify false negative as one of the challenges faced by the analyst. FN's are generally the result of a detections system inability to identify true security events posing a challenge for the analysts [39, 3]. Analysts have to rely on other signs on the network, for example, using behavioural analytical technique to identify malicious activity.
- **Sophisticated Attacks** – (P3, P4, P6, P8, P12, P13, P14 and P15) report sophisticated attacks as another challenge for analysts. Modern-day attacks can be hard to detect, especially given the complexity and stealthy methods used. Zhong et al. [3], suggest that the complexity pose challenges to analysts ability to spot them among complex and large data sets. Analysts have to rely on experience to thwart attacks when the attacker evades existing technical controls [40].

- **Incident Handling/Incident Management Complexity** – Responding to incidents is a key responsibility of analysts, and all incidents need to be handled in a manner that reduces further damage [4,15]. Along with this, analysts are also under time pressure during incident handling [15]. Identifying an attack is one thing; handling the attack through the incident handling process is another [36]. Both P4 and P10 suggest that detecting and managing security incidents (attack) is crucial for the success of a SOC. Incident management typically involves engaging with (or escalations to) other teams, internal or external to the organisation, to ensure that the impact of any attack is minimised or removed [41]. The complexity of incident handling can be daunting for less experienced analysts which means they rely on the guidance of experienced analysts. With studies suggesting SOCs struggling to retain experienced analysts, handling complex incidents becomes a challenge [10].
- **Skills/Experience Shortage –** (P3, P4, P5, P12 and P15) highlight skills and experience shortages are among the challenges facing the analysts. The rapid turnover of analysts means SOCs struggle to retain their most experienced and qualified analysts [1]. This creates a challenge for less experienced analysts as the opportunity to learn from experienced analysts becomes an issue. The dynamic nature of cyber threats means that unless analysts receive periodic training, either in-house or off-site paid training, they are unlikely to possess that skills required to beat off an attacker [7].
- **Inadequate Communication between Teams –** P1 reports inadequate communicate between analysts as one of the challenges in SOCs [5]. Hámornik & Krasznay [15],explains that communication and information sharing is vital to the success of a SOC although they argue that team members generally do not have time to communicate when they are under pressure. The lack of effective communication between the team impact on the team's performance [15]. Sundaramurthy et al. [7], state that SOCs must work towards addressing the lack of communication so that analysts do not feel left behind or isolated.
- **Tacit Knowledge** – The problem with tacit knowledge is that it is not limited to SOC environment as many professions also have a similar issue [42]. However, within a SOC environment, P2 and P11 highlight that tacit knowledge can hinder or slow down the investigation in the SOC. Equally, P7 explains that one of the issues with tacit knowledge is that, experienced analysts are unable to clearly explain reasons behind their actions for less experienced analysts to learn. One approach to addressing this may be for SOCs to have playbooks or run books along with well-documented processes that less experienced can draw on to aid decision making in SOCs. Further research into analysts decision-making process is required.
- **Manual and Repetitive Processes** – (P1, P2, P4, P5, P6, P7, P9 and P15) identified manual, repetitive and mundane step by step processes used by

some SOCs as causing dissatisfaction among the SOC analysts [7, 5, 44]. Following rigid processes can also hinder analysts creativity in the SOC [7]. Other problems with manual processes and analysis is that, they are highly inadequate for an enterprise organisation and businesses need to gear efforts towards automation [6,7]. The use of SIEM (Security Information and Event Management) technologies along with security event visualisation systems can ease off some of the burden associated with manual and repetitive processes [1,2].

- **Workloads** – Sundaramurthy and his colleagues [43],argue that analysts are confronted with more alerts than they can investigate. This view is supported by Feng et al. [38], who suggest that increased workload is mainly due to the overwhelming number of alerts analysts have to process. P3, P6, P7, P10, P9, P13, P14 and P15 all identify workload as a major challenge faced by analysts. Previous studies suggest that increased workload also makes it difficult for analysts to maintain situational awareness, vigilance and attention [4]. Lif and Sommestad [4],posit that workload impacts on analysts monitoring, analysis and response capabilities. They further argue that attention has an impact on operators (analysts) response time and so are eye movement when it comes to vigilance. These human factors that lead to poor performances are often less investigated or even measured to see how performance can be tracked and improved.
- **Analyst Burnout** – P2 and P3 identify burnout as a major challenge facing SOC analysts. Burnout phenomenon is an active area of research for many researchers [7,14]. The consensus amongst researchers is that burnout is the result of multiple organizational, environmental and human factors such as alert fatigue, stress, workload and anxiety which in turn lead to turnover among analysts [15,44].
- **Assessment Methods for Analysts** – SOC managers, usually expect good operational performance from their analysts as noted by P1 and P2 [5,7]. However, studies suggest a lack of adequate metrics and measures for assessing the performance of analysts. The problem here is that in some cases, analysts and managers do not agree on how performance needs to be measured, and managers have difficulty in devising good metrics. Sundaramurthy et al. [7],state that analyst benefits from good metrics because their bonuses and promotions are decided using metrics. Analysts expect objective metrics that takes several aspects of their work into consideration. The present lack of adequate metrics creates an avenue for further studies, as noted by P1.

Performance metrics and measures in use

Research question 2 asked what metrics exist to measure the performance of a SOC analyst. It is worth noting that studies that investigate the performance of

SOC capabilities and SOC maturity levels are complementary to but distinct from our objective [1,2]. Our focus is on the analyst performance metric, i.e. metric that measures how well the analyst performs. We noted that there are limited metrics for measuring analyst performance and this has been attributed to the difficulty in devising a useful metric, as managers do not even know what the right metric should be [7]. Ten of the selected papers (P1, P2, P5, P6, P7, P9, P11, P12, P13, P14) identify and reports on various metrics that are frequently used to measure analysts performance.

As pointed out earlier, authors do not always make the distinction between metrics and measures and use the terms interchangeably. To that end, we grouped existing assessment methods into quantitative and qualitative metrics/measures. The quantitative metrics/measures are less open to interpretation and provide concrete measures, unlike the qualitative metrics that uses non-numerical and interpretive approach. The quantitative metrics identified are:

- **Time to Detect an Incident (TTD) or Average Time to Detect (ATTD)** – This metric focuses on the delta (time) between an issue occurring and the analyst noticing it as identified in P1 and P11. It takes into consideration the time an alert is detected by a detection tool, such as an Intrusion Detection System (IDS) or a SIEM, and the time that the analyst discovers it.
- **Average Time Taken to Respond (ATTR)** – ATTR focuses on the time taken by an analyst to respond to an incident as reported in P12 and P14. Unlike ATTD, ATTR assesses response time rather than detection time. Responding may entail specific action such as reconfiguring a network to stop any threat. Some authors refer to this as the Average Total Time for Alert (avgTTA) Investigation [47]. Others refer to this as the time taken to investigate a customer under attack [39]. The time-based metrics focus on analysts reaction times, in terms of how quick they respond or detect an incident.
- **Number of Alerts Analysed/Unanalysed by an analyst at the end of a shift** – This measure, focuses on counting the number of alerts processed by the analysts as identified in P6 and P14. These metrics do not take into consideration the complexity of the alert [43].
- **The number of tickets closed per day** – This metric merely counts the number of tickets closed by the analyst at the end of the day (P7, P9). These are incidents that have been resolved with no further actions required and have therefore been closed by the analyst. This metric can be adjusted and taken at the end of the week or even at the end of the month to show the performance of an analyst as suggested by Onwubiko [6].
- **The number of incidents detected within a specific timeframe** – This metric attempt to capture the number of real events identified by the analyst over a certain period as reported in P5. Closely associated with the number of incidents detected, is a metric that counts the number of

false positives, number of false negatives, true positives and true negatives. Onwubiko [6],suggest that metrics such as the number of false positives, number of false negatives, true positives and true negatives as a useful metrics that can be used by SOC managers to measure the performance of analysts. Jaquith [45],explains that metrics that are expressed in numbers or percentages are better than subjective measures because subjective measures that can vary from one person to other.

- **Time spent on operations by the analyst** – Operations in this situation refers to specific tasks that have been assigned to the analyst by their manager (P2). Analysts are measured on time it takes to complete these tasks [5]. This kind of metrics are dependent on the functions expected of analysts and may well vary from one SOC to another. We argue that the different functions and tasks expected from analysts could be one of the reasons why researchers find it difficult to devise an objective metric.
- **Time spent on each ticket** – Some authors associate this with the time it takes the analyst to create tickets (P1). Naturally, some tickets take longer than others, depending on the nature and complexity of the incident involved [5]. Research suggests that analysts despise these kinds of time-based metrics [7], however, to the best of our knowledge, there is currently no study that investigates how to improve existing measures from the viewpoint of an analyst.

Whereas the above metrics focus on quantitative measures, there are other analyst performance metrics based on qualitative (subjective) measures. Nevertheless, both categories of metrics provide an empirical measure as they are based on observations and experiences of analyst [46]. Qualitative metrics identified are:

- **A measure of the competency and experience of the analyst** – Some SOC researchers uses questionnaires or simulated exercises to assess the experience and competency of analysts. For example, Schinagl, Schoon and Paans [1],in P4 used a questionnaire to gather information on the reported experiences of analysts as part of evaluating the overall effectiveness of a SOC [1]. Others writers such as McClain et al. [10],employ cyber training exercises to assess the competencies of analysts based on the outcome of their performance.
- **The Use of Success Stories** – The need to justify the value of SOCs and analyst's performance has led to some SOCs using 'success stories' as reported by P7. P1 explain that success stories are used to demonstrate the achievement/s of analysts and the impact of implementing a specific technical solution. An example of a success story for the analysts may be the detection of a true event based on a use case designed by the analysts. However, this type of qualitative measurement often means that people

without security background do not generally understand what the achievement means [5].

- **The Quality of Incident Reports** – Analysts are expected to generate a report as part of their investigation and are measured on the quality of the report (P6 and P13). However, Zhong et al. [47, 44] argue that the volume of alerts impedes on analysts ability to generate a high-quality incident report. Notwithstanding, for such a measure to be effective, the useful pieces of information analysts need to collect must to be communicated to analysts and should be standardised across the team.
- **Quality of Analysis** – Shah et al. [3],suggest that in addition to the need to identify threats promptly, analysts also need to undertake quality analysis. While this may be an accurate statement, the problem with this kind of measurement is that the term 'quality' is subjective and makes it difficult to define such a metric [45].

Mapping metrics and challenges

The purpose of RQ3 was to examine the mapping between the challenges faced by analysts and metrics for measuring analysts performance. Hart [20],state that mapping denotes the linkage between ideas, data and concepts from existing literature. With this in mind, we sought to investigate the relationship between analysts performance metrics and the challenges they face. A conclusion drawn from the papers reviewed was that some authors mention analysts performance metrics; but do not discuss how these metrics capture's analysts efforts (performance) as they address some of the challenging aspects of their work [1,6]. Others, however, attempt to show the link between the challenge faced by analyst and existing metrics for measuring the performance. For example, Shah et al. [48],point out how large volume of alerts impede on analysts reaction time (time to detect). To our surprise, Sundaramurthy and his colleagues actually identify the lack of an objective performance metric as one of the challenges facing SOC analysts [5,7]. We believe this is a clear research gap that future work can address.

We noted that, although there are metrics for assessing the performance of analysts as they tackle some of the challenging aspects of their work; existing metrics are disjointed as they tend to focus on different challenges or analysts' tasks and does not give a holistic picture [6]. This finding, in a way, confirms the concerns raised by analysts in the anthropological study of SOCs conducted by Sundaramurthy et al. [7] in which analysts pointed out how many of their efforts are not taken into consideration under existing metrics. Based on our findings and insights of existing literature, we created a mapping between the challenges faced by analysts and the coverage provided by existing metrics Figure 4.

The mapping provides a better understanding of the topic under study as it allows the relationship between the ideas to be expressed [49]. In addition, we hope that the mapping will give clarity on how the various concept relates. Our mapping is based on papers used for the SLR and other scientific articles on

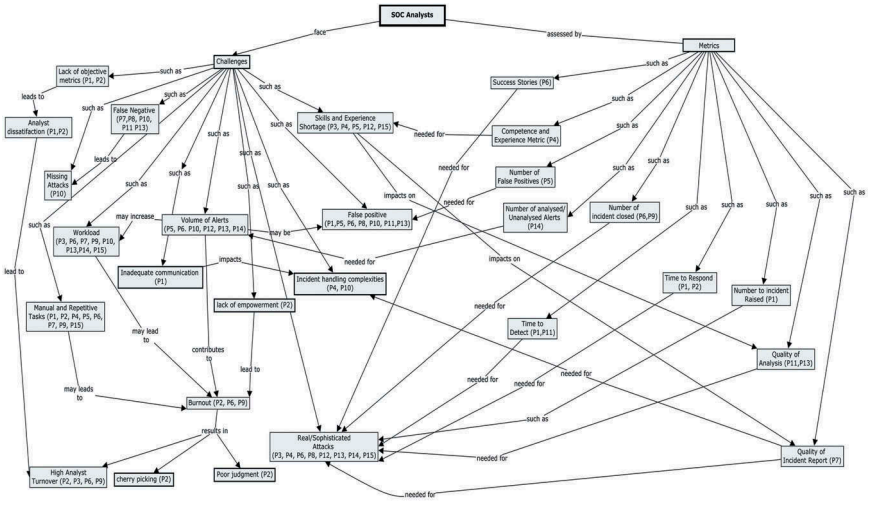

Figure 4. Linkage between challenges faced by analysts and analysts' performance metrics.

SOCs [1,5–7,12]. Hart [20],suggest six ways of mapping ideas and representing knowledge. These are feature maps, variable matrix, tree constructions, content maps, taxonomic maps and concept maps.

Definitionally, according to Hart [20], a concept map is useful for constructing and showing the relationship between ideas and practice. It can also express the relationship between theory and practice. As per the format of a typical concept mapping, our mapping is in hierarchical structure starting with the SOC analysts at the top. This is followed by the two key concepts: challenges (on the left of the diagram) and metrics (on the right of the diagram). References of papers that mention specific challenges and/or metrics are listed and shown in brackets next to each concept in the form of P1, P2, P3 etc. Further details of each paper can be found in Appendix A on Table A1. The metrics reported in Figure 4 can be split into two categorizes time-based metrics and raw cardinal numbers. The time-based metrics focus on reaction time, for example, the time it takes an analyst to detect or respond to an incident. On the other hand, raw cardinal numbers count the number of objects, for example, the number of incidents raised or closed.

Looking at Figure 4, it is evident that several metrics exist to measure analysts' efforts as they tackle many of the challenging aspects of their work. A one-way arrow is used to illustrate the relationship between the metrics and the challenges. The majority of the metrics focus on analysts' efforts in addressing their operational objective/task or goal, for example, the time it takes an analyst to detect a real attack or false positive. There are, however, some challenges reported in Figure 4 with no associated metrics, for example, analysts' burnout. Given that, one of the key responsibility of analysts is to detect cyber-attacks, it is not surprising that most of the metrics are geared towards measuring analysts' efforts

in detecting sophisticated attacks. Indeed, all the metrics showed in Figure 4 can be used to evaluate how well the analysts are performing, albeit they are disjointed and unless a SOC implements multiple metrics, it will be hard to get a holistic view of analysts' effort. Notwithstanding, measuring human factors such as analysts situational awareness, vigilance and attention are also important to get a holistic view of analysts performance [4].

Discussion

Although SOCs have been an active research area, the challenges faced by analysts and performance metrics for analysts are usually mentioned by researchers in passing and are rarely the main focus. This is discouraging because challenges faced by analysts impacts on the performance of the SOC [44]. Identification of specific challenges faced by analysts will provide SOC experts with an opportunity to learn and facilitate the development of novel approaches to helping analysts address these challenges. Likewise, measuring the performance of an analyst is important because anything that is not measured cannot be managed [9]. From a practical perspective, an objective performance metric can be used by the analyst for self-assessment to establish how well they are contributing to the team's objective. SOC managers can also use objective performance metrics to evaluate analysts' performance and to motivate them [7].

Many of the challenges faced by the analyst pointed out in the papers reviewed, play into the hands of an attacker. For example, over 40% of the papers reviewed reported the volume of alerts received by an analyst as a critical issue. Although collecting system events logs can provide valuable information about an attacker's activities, in practice large volume of alerts also means that the analysts have to go through thousands of alerts to detect a single true attack if any [7]. Attackers can easily blend in among the mist of several logs. Recommendations such as collecting essential logs, designing useful use cases (UC's) and using pre-defined correlation rules in SIEM solutions, do not seem to address this challenge [50, 44]. While it is acknowledged that analysts cannot possibly investigate all alerts and that some level of automation is required, tuning policies can help analysts to manage alert volumes. Interestingly, to the best of our knowledge, analysts coping strategies when it comes to managing a large volume of alerts have not been studied or addressed before in literature.

We observed that FPs wastes analysts time and has an impact on the overall performance of the SOC [51]. 47% of the selected papers identify FPs as a major challenge facing analysts. Analysts have a responsibility to filter out noise to optimize their performance. Onwubiko [6] argues that an effective SOC must reduce the number of false positives presented to the analyst. He asserts that a performance metric that consistently shows false positives outnumbering true

positives indicate the need for policy tuning or training of the analyst. However, policy tuning and filtering to reduce FPs is a time-consuming activity [15]. Notwithstanding, unless analysts are measured on the number of FP tickets raised, managers will not know those that need training. Future metrics, therefore, must take this into consideration.

Another area of concern is analyst burnout, which research shows lead to high analyst turnover. According to Sundaramurthy et al. [7,12], negative factors such as low skills, the lack of empowerment, low growth and low creativity in SOCs lead to analyst burnout. They propose a model to explain the burned-out phenomena among analysts. However, the completeness of the model was not adequately verified due to the lack of analysts to participate in the study. Besides, evidence from current literature shows that there are other challenges faced by analysts that were not captured in their work. For example, dealing with sophisticated attacks and false positives [52]. Notwithstanding, none of the papers reviewed provides a comprehensive overview of the challenges faced by the analyst. We argue that further research is needed to fill this gap and to validate prior work. The paper at hand is a stepping stone towards this goal.

When it comes to measuring analyst performance, our review suggests that various metrics exist for doing this; however, some authors argue about their completeness and objectivity and make a case for the need for further research in this area [5]. There are many aspects of analysts work or challenges that are not taken into consideration to give a holistic picture of their performance in a SOC [7]. We noted that existing performance tends to focus on analysts reaction time, for example, time to detect an incident [7,39,47,48] or the frequency at which a particular analyst task is carried out; in numerical terms [5–7]. The frequency in this situation refers to how often the data is collected or reported [53]. Responsibilities of analysts are well documented by various studies [1,6,54]. For example, analysts are expected to create Use Cases (UC's) to detect attacks or modify UC's, yet in the examined literature we did not come across an objective metric that takes use case creation into consideration [6].

Sundaramurthy et al. [7],highlight the concerns amongst analysts with regard to some of the time-based metrics. For example, they claim that an analyst argues that a metric that measures performance based on the time taken to resolve an incident does not take into considerations other operational tasks. Likewise, some of the existing time-based measures are also theoretical concept and not practical in many SOCs. For example, in their work 'A methodology for ensuring fair allocation of CSOC effort for alert investigation', Shah et al. [39], assumed that a SOC would employ analysts with similar capabilities (expertise). With this assumption in mind, they designed a time-based measure to compute analyst hours per day on their tasks. However, in practice, it is not practical for any SOC to have analysts with the same capabilities [39]. SOCs, therefore, employ analysts with varied skills and experience [5]. Also, skills shortage and the financial cost of hiring experienced analysts makes this unachievable.

Metrics that focus on counting the number of specific tasks carried out by analysts have been cited as useful for SOC managers [6]. However, these metrics also have their limitations. For instance, metrics that count the number of security incidents raised or closed by an analyst do not take into consideration the complexity or priority of the incident [43]. In fact, such a metric does not provide enough information to differentiate two or more analysts raising the same number of incidents, assuming one is raising critical incidents, and another is raising false positives or lower priority alerts. Sundaramurthy et al. [5],stress that priority should be given to alerts that pose a direct threat. A metric that merely counts the number of incidents raised by analysts as shown in Figure 4 may suggest that the analysts are on par. However, in reality, some analysts may choose to raise or close a high quantity of easy tickets to look good on such a metric [43]. Shah et al. [39],suggest that alerts processed by analysts are usually classified as low, medium and high severity. It would make sense for a performance metric to take into account the priority or severity of the incident raised rather than treating all incident as the same. We are not advocating for focusing solely on high priority events/alerts and suppressing everything else. But rather, we argue that a good metric should have features that make such distinctions; taking into consideration multiple factors to help SOC managers and analysts to get a holistic view.

It is clear from our review that, there is a need for improvement of existing analyst's performance metrics. In-fact existing metrics are not sustainable because of the frustration and dissatisfaction it causes among analysts [7,43]. Although researchers have used ethnographic methods, case studies, grounded theory and anthropology to study analysts, these methodologies do not necessarily seek to devise strategies to address analysts problems and challenges [20,55].

An alternative methodology such as design science can be used alongside case study to facilitate the design or improvement of existing analyst metrics. However, given that a SOC is unique to its organisation [1], research is needed to ascertain the feasibility of designing a universal set of metrics that can be used by analysts working in different SOCs. Indeed, the role of analysts can be broad and varied making it difficult to measure every aspect [10]. Guidance on designing a useful performance metric provided by the National Institute for Standards and Information Technology [53] and the International Organisation for Standardization/Electrotechnical Commission (ISO/IEC 27004) can be used to validate a new proposed set of metrics.

A limitation of this study is that we did not contact any of the authors of the selected papers, so the interpretation presented in this work is based on our understanding. One challenge encountered during the SLR process relates to data extraction and synthesis due to the different approaches used by the various writers in presenting their studies. We, therefore, had limited options on how to present our findings and had to rely on narrative synthesis to present the results.

Conclusion

This paper presents the findings of a SLR conducted to identify the challenges faced by SOC analysts and existing metrics for measuring analyst performance as they address the challenging aspects of their work. The SLR also investigate the mapping between the challenges faced by analysts and coverage provided by existing analysts performance metrics. One hundred and twenty-one (121) papers were initially selected as part of our SLR process; however, only 15 studies were included, based on our review protocol and criteria.

In this study, we identified twelve (12) challenges faced by analysts and report them as: the volume of alerts presented to the analyst; the number of false positive alerts; false negatives; sophisticated attacks; incident handling/incident management complexity; skills/experience shortage; inadequate communication between teams; tacit knowledge; manual and repetitive processes; workloads; analysts burnout and the lack of adequate metrics and measures for assessing the efforts of analysts. We also identified the following metrics and measures for assessing the performance of analysts: time to detect an incident/average time to detect an incident, average time taken to respond to an incident, number of alerts analysed/unanalysed by an analyst at the end of a shift, the number of tickets closed per day, the number of incidents detected within a specific timeframe, time spent on operations by the analyst, time spent on each ticket, a measure of the competency and experience of the analysts, success stories, the quality of incident reports and the quality of analysis.

Our findings suggest that there are several areas of an analyst's work that can be measured to give a comprehensive picture of the work of an analyst. Our mapping of the challenges faced by analysts and the coverage provided by existing metrics also revealed that there are some challenges with no associated metrics, for example, the burnout phenomenon. Such a metric will be useful for SOC managers who may want to measure burnout amongst analysts.

This paper consolidates and synthesizes existing knowledge on the challenges faced by analysts along with existing metrics for measuring analysts performance. A key lesson learnt is that effort to investigate and understand intervention strategies to address the challenges faced by the analysts are lacking. Furthermore, this study has revealed that analysts' performance is not necessarily measured based on their efforts in addressing the challenges they face. Rather analysts' performance metrics are based on effort in achieving their tasks/functions amid the challenges they face.

This paper suggests that more research is needed on the human, organisational and environmental factors that impact on analysts performance. Additionally, we argue for an improvement to existing measures and metrics for assessing the performance of analysts. The areas that have not been adequately addressed by existing studies and therefore are in need of further research are:

- A novel and an objective approach to measuring the performance of a SOC analyst based on multiple factors derived from their work;
- A thorough exploration of the challenges that analyst face within a SOC and how these challenges can be addressed from a native (analysts) perspective to improve their performance.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Enoch Agyepong is a Researcher at the School of Computer Science and Informatics, Cardiff University. He holds a Master's Degree in Advanced Security And Digital Forensics from Edinburgh Napier University. His research interest is in Cyber Security and Security Operation Centers.

Dr Yulia Cherdantseva is a lecturer at the National Software Academy at Cardiff University. She specialises in Cyber Security, Secure Business Process Design and Risk Assessment. She holds a PhD in Computer Science and an MSc (Hons) in Business Information Systems Design, Russia.

Dr Philipp Reinecke is Researcher and Lecturer in Cybersecurity, Performance, and Dependability at School of Computer Science and Informatics at Cardiff University, UK. He holds a PhD in Computer Science from Freie Universität Berlin and an MSc in Computer Science from Humboldt University of Berlin.

Pete Burnap is a Professor of Data Science and Cybersecurity at Cardiff University. He is the Director of Cardiff's NCSC/EPSRC Academic Centre of Excellence in Cyber Security Research (ACE-CSR). He holds a PhD in Computer Science from Cardiff University. https://burnap.org/

ORCID

Enoch Agyepong http://orcid.org/0000-0003-3280-1745

References

[1] Schinagl S, Schoon K, Paans R. A framework for designing a security operations centre (SOC). 48th Hawaii International Conference on System Sciences; IEEE; 2015. p. 2253–2262. doi: 10.1109/HICSS.2015.270.

[2] Jacobs P, Arnab A, Irwin B. Classification of security operation centers. Information Security for South Africa; IEEE; 2013. p. 1–7. doi: 10.1109/ISSA.2013.6641054.

[3] Zhong C, Yen J, Liu P, et al. Automate cybersecurity data triage by leveraging human analysts' cognitive process. 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 Security. New York, USA: IEEE; 2016. p. 357–363. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.41.

[4] Lif P, Sommestad T. Human factors related to the performance of intrusion detection operators. 2015.

[5] Sundaramurthy SC, Case J, Truong T, et al. A tale of three security operation centers. Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW '14; Scottsdale, Arizona: ACM; 2014. p. 43–50. doi: 10.1145/2663887.2663904.

[6] Onwubiko C. Cyber security operations centre: security monitoring for protecting business and supporting cyber defense strategy. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA); London, UK: IEEE; 2015. p. 1–10. doi: 10.1109/CyberSA.2015.7166125.

[7] Sundaramurthy SC, Bardas AG, Case J, et al. A human capital model for mitigating security analyst burnout. Symposium on Usable Privacy and Security; Ottawa, Canada; 2015. p. 347–359.

[8] Zhong C, Lin T, Liu P, et al. A cyber security data triage operation retrieval system. Comput Secur. Elsevier Ltd. 2018a;76:12–31.

[9] Kaplan RS. Measuring performance : expert solutions to everyday challenges. Boston: Harvard Business Press; 2009.

[10] Mcclain J, Silva A, Emmanuel G, *et al*. Human performance factors in cyber security forensic analysis. Procedia Manuf. 2015;3:5301–5307.

[11] Aijaz L, Aslam B, Umar K. Security operations center — A need for an academic environment. World Symposium on Computer Networks and Information Security (WSCNIS); 2015 Sept 19–21; Hammamet, Tunisia; 2015. p. 1–7.

[12] Sundaramurthy SC, Wesch M, Ou X, et al. Humans are dynamic-our tools should be too. IEEE Internet Comput. 2017a;21(3):40–46.

[13] Sundaramurthy SC, Wesch M, Ou X, et al. Humans are dynamic. Our tools should be too. Innovations from the anthropological study of security operations centers. IEEE Internet Comput. 2017b;1. DOI:10.1109/MIC.2017.265103212

[14] Hull JL. Analyst Burnout in the Cyber Security Operations Centre - CSOC: A phenomenological study [Doctoral dissertation]. Colorado Springs (CO): Colorado Technical University; 2017.

[15] Hámornik PB, Krasznay C. A team-level perspective of human factors in cyber security: security operations centers. Cham: Springer; 2017. p. 224–236. DOI:10.1007/978-3-319-60585-2_21.

[16] Andrade RO, Yoo SG. Cognitive security: A comprehensive study of cognitive science in cybersecurity. J Inf Secur Appl. 2019;48:102352.

[17] Black PE, Scarfone K, Souppaya M. Cyber security metrics and measures, handbook of science and technology for homeland security. 2009.

[18] Sambasivan M, Abidin Mohamed Z, Nandan T. Performance measures and metrics for e-supply chains. J Enterp Inf Manage. Emerald Group Publishing Limited. 2009;22 (3):346–360.

[19] Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. 2007.

[20] Hart C. Doing a literature review: releasing the research imagination. 2nd ed. London: Sage Publications Ltd; 2018.

[21] Silva RLS, Neiva FW. Systematic literature review in computer science-a practical guide. Relatórios Técnicos Do DCC/UFJF. 2016. DOI:10.13140/RG.2.2.35453.87524

[22] University of Liverpool. 2018. Which are the best databases for computer Science? - Library help. [cited 2019 Feb 15]. Available from: https://libanswers.liverpool.ac.uk/faq/49363

[23] Kitchenham B, Brereton P. A systematic review of systematic review process research in software engineering. Inf Software Technol. Elsevier B.V. 2013;55(12):2049–2075.
[24] Cherry G, Dickson R. Defining my review question and identifying inclusion and exclusion criteria. In: Boland A, Cherry G, Dickson R, editors. Doing a systematic review: a student's guide. 2nd ed. London: Sage publications Ltd; 2017. p. 43–50.
[25] Dybå T, Dingsøyr T. Empirical studies of agile software development: A systematic review. Inf Software Technol. 2008;50(9–10):833–859.
[26] Moher D, Liberati A, Tetzlaff J, et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Ann Intern Med. American College of Physicians. 2009;151(4):264.
[27] Usman M, Mendes E, Weidt F, et al. Effort estimation in agile software development : A systematic literature review. Proceedings of the 10th international conference on predictive models in software engineering; 2014 Sept 17–17; Torino, Italy; 2014. p. 82–91. doi: 10.1145/2639490.2639503.
[28] Lee CJ, Sugimoto CR, Zhang G, *et al*. Bias in peer review'. J Am Soc Inf Sci Technol. Wiley-Blackwell. 2013;64(1):2–17.
[29] Maynard C. Personal Bias in Peer Review. Med Care. 2018;56(7):643.
[30] Critical Appraisal Skills Programme. CASP Checklist: 10 questions to help you make sense of a systematic review. 2018.
[31] Cherry G. Reviewing qualitative evidence. In: Boland A, Cherry G, Dickson R, *et al*. (editors.) Doing a systematic review: a student's guide. 2nd ed. London:Sage publications Ltd; 2017. p.195–221.
[32] Dos Santos ACC, Delamaro ME, Nunes FLS. The relationship between requirements engineering and virtual reality systems: A systematic literature review. Proceedings - 2013 15th Symposium on Virtual and Augmented Reality, SVR 2013 May 27-30; Cuibá, Mato Grosso, Brazil–; 2013. p. 53–62. doi: 10.1109/SVR.2013.52.
[33] Boland A, Cherry MG, Dickson R. Doing a systematic review : a student's guide. London: SAGE; 2017.
[34] Hewlett-Packard (2013) *5G/SOC: SOC generations -HP ESP security intelligence and operations consulting services - business white paper*.
[35] Miloslavskaya N (2016) Security operations centers for information security incident management. Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016 Aug 22–25; Vienna, Austria; p. 131–138. doi: 10.1109/FiCloud.2016.26.
[36] SANS Institute. SEC504: hacker techniques, exploits, and incident handling. Boston: The SANS Institute; 2018.
[37] Kwon T, Song JS, Choi S, et al. VISNU: A novel visualization methodology of security events optimized for a centralized SOC. 13th Asia Joint Conference on Information Security (AsiaJCIS); 2018 Aug 8–9; Guilin, China; IEEE; 2018. p. 1–7. doi: 10.1109/AsiaJCIS.2018.00010.
[38] Feng C, Wu S, Liu N A user-centric machine learning framework for cyber security operations center. IEEE International Conference on Intelligence and Security Informatics (ISI); 2017 July 22–24; Beijing, China; IEEE; 2017. p. 173–175. doi: 10.1109/ISI.2017.8004902.
[39] Shah A, Ganesan R, Jajodia S. A methodology for ensuring fair allocation of CSOC effort for alert investigation. Int J Inf Secur. Springer Berlin Heidelberg. 2018;18:1–20.
[40] Falk E, Repcek S, Fiz B, et al. VSOC - a virtual security operating center. IEEE Global Communications Conference, GLOBECOM 2017 – Proceedings; Marina Bay, Singapore; 2017. p. 1–6. doi: 10.1109/GLOCOM.2017.8254427.

[41] Kowtha S, Nolan LA, Daley RA Cyber security operations center characterization model and analysis. IEEE International Conference on Technologies for Homeland Security, HST 2012 Nov 13–15; Waltham, Massachusetts; IEEE; 2012. p. 470–475. doi: 10.1109/THS.2012.6459894.

[42] Girard J, Girard J. Defining knowledge management: toward an applied compendium. Online J Appl Knowl Manage Publ Int Inst Appl Knowl Manage. 2009;3(1).p. 1–20.

[43] Sundaramurthy SC, McHugh J, Ou X, 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. The Symposium On Usable Privacy and Security (SOUPS); USA: USENIX; 2016. p. 237–251.

[44] Zhong C, Yen J, Liu P, et al. Learning from experts' experience: toward automated cyber security data triage'. IEEE Syst J. 2018b; p. 1–12. DOI:10.1109/JSYST.2018.2828832.

[45] Jaquith A. Security metrics: replacing fear, uncertainty, and doubt. Boston: Pearson Education, Inc; 2007.

[46] Hayden L. IT security metrics : a practical framework for measuring security and protecting data. London: McGraw Hill; 2010.

[47] Shah A, Ganesan R, Jajodia S, et al. Understanding trade-offs between throughput, quality, and cost of alert analysis in a CSOC. IEEE Trans Inf Forensics Secur. IEEE. 2018b; 14 (5) . p. 1155–1170. DOI:10.1109/TIFS.2018.2871744.

[48] Shah A, Ganesan R, Jajodia S, *et al*. Adaptive reallocation of cybersecurity analysts to sensors for balancing risk between sensors. Serv Oriented Comput Appl. Springer London. 2018a;12(2):123–135.

[49] Creswell JW, Creswell JD. Research design : qualitative, quantitative, and mixed methods approaches. London: Sage Publications; 2018.

[50] Scarabeo N, Fung BCM, Khokhar RH. Mining known attack patterns from security-related events. PeerJ Comput Sci. 2015;1:e25.

[51] Chamiekara GWP, Cooray MIM, Wickramasinghe LSAM, et al. AutoSOC: A low budget flexible security operations platform for enterprises and organizations. National Information Technology Conference, NITC 2017; 2017 Sept 14–15; Colombo, Sri Lanka; 2017. p. 100–105. doi: 10.1109/NITC.2017.8285644.

[52] Graf R, King R Secured transactions technique based on smart contracts for situational awareness tools. 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017 Dec 11–14; Cambridge, UK; 2017. p. 81–86. doi: 10.23919/ICITST.2017.8356352.

[53] Chew E. Swanson M, Stine K, et al. Performance M NIST special publication 800-55 revision 1. Measurement guide for information security, National Institute of Standards and Technology, US Department of Commerce. Computer Division, Gaithersburg, MD ;2008. DOI: 10.6028/NIST.SP.800-55r1.

[54] D'Amico A, Whitley K. The real work of computer network defense analysts. In: Goodall JR, Conti G, Ma K, editors. VizSEC 2007 : proceedings of the workshop on visualization for computer security. Springer Berlin Heidelberg; 2008. p. 19–37.

[55] Paul CL . Human-centered study of a network operations center: experience report and lessons learned. Proceedings of the ACM Workshop on Security Information Workers; Scottsdale, Arizona; 2014. p. 39–42. doi: 10.1145/2663887.2663899.

Appendix A

Table A1. Data extraction form.

Author(s) Year of Publication [Reference] (Paper)	Method of Investigation	Data Collection Method	Challenges faced by SOC Analyst (RQ1)	Performance Metric for SOC Analyst Identified (RQ2)
[5] (P1)	Anthropology	*Direct daily observation of analysts. *Fieldwork data notes. *Interviews	*Maintaining effective communication between teams with the SOC. *False positives.	*Counting number of tickets actioned by the analyst. *Amount of time taken to raise a ticket.
[7] (P2)	Anthropology Grounded Theory Method (GT)	*Direct daily observation of analysts. *Fieldwork data notes. *Interviews	*Frequent staff turnover. *Analyst burnout.	*Time spent on operations by the analyst. *Time spent on creating tickets.
[10] (P3)	Case Study	*Questionnaire-based assessments. *Behavioural performance based on human-machine transactions	*Workload *Limited skills *Analyst turnover	*Competence of analyst.
[1] (P4)	Case Study	*Researcher designed questionnaire	*Identifying complex attacks.	*Measure of competence and experience
[6] (P5)	Not listed	None	*Tuning of false positives. *Volume of alerts.	*Number of False Positives *Number of False Negatives *Number of True Positives and *Number of True Negatives.
[3] (P6)	Case study	An experiment based on captured traces of analysts' operations in performing data triage tasks.	*Volume of alerts and false positives *Workload and fatigue *Issue with false negative and sophisticated attacks.	Generating high quality incident report.
[43] (P7)	Anthropology	*Direct daily observation of analysts.	*Burnout *Workload *Repetitive tasks	*Number of incidents resolved/closed *Success stories
[52] (P8)	Not stated	*Experiments based on randomly selected cyber incidents reports.	*Finding true attack in large and complex data set. *False positives	None
[13] (P9)	Anthropology	*Interviews and *Fieldnotes	*Analyst burnout *Manual and mundane tasks. *Restrictive standard operating procedures.	*Number of tickets closed per day.
[38] (P10)	Case Study	*Experiment using machine learning algorithm to calculate a risk score of users' activities on the network. The analyst can then prioritise their work based on user risk score.	*Number of alerts presented to the analyst can be overwhelming *False positive *Missing real attacks and compromised host.	None Reported

(*Continued*)

Table A1. (Continued).

Author(s) Year of Publication [Reference] (Paper)	Method of Investigation	Data Collection Method	Challenges faced by SOC Analyst (RQ1)	Performance Metric for SOC Analyst Identified (RQ2)
[47] (P11)	Case study	*Experimentation using simulation algorithms and a mathematical model to compute total time of alert investigated by an analyst per hour.	*False positive *False negatives	*Average Total time for alert (avgTTA) investigation. *Time to detect an incident. *Quality of analysis
[39] (P12)	Case study	*An experiment. Proposes a dynamic weighted alert queuing (DWQ) mechanism to ensure that analyst investigate high priority alert first and a fair allocation of CSOC effort.	*Dealing with higher than expected alerts. *Not enough analyst to investigate all alerts. *Zero-day alerts/ attacks	*Time taken to investigate customer under attack.
[44] (P13)	Case study	*Experiment using captured traces of analysts' cognitive processes of data triage. (Graph based trace mining)	*Volume of alerts *False positives *Detecting true incident *Workloads	*Number of quality incident report
[48] (P14)	Case studies	*Simulation/Experimental activity based on a novel mathematical model to re-allocate analysts to sensors to reduce backlogs of alerts from sensors.	*Inability to analyse all presented to the analyst. *Balancing workload due to the number of alerts. *Dealing with a zero-day attack.	*Average time taken to raise or analyse an incident. *Number of alerts analysed/ unanalysed by an analyst at the end of a shift.
[15] (P15)	Case Study	*Semi- Structured *Interviews with SOC experts.	*Skills shortage *Complex Attacks	None