Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A systematic method for measuring the performance of a cyber security operations centre analyst

Enoch Agyepong*, Yulia Cherdantseva, Philipp Reinecke, Pete Burnap

School of Computer Science and Informatics, Cardiff University, United Kingdom

ARTICLE INFO

Article history:
Received 27 December 2021
Revised 7 July 2022
Accepted 14 October 2022
Available online 21 October 2022

Keywords:
Security operations centre
Analysts' metrics
Performance metrics
Analysts' evaluation
Key performance indicators
Analytic hierarchy process

ABSTRACT

Analysts who work in a Security Operations Centre (SOC) play an essential role in supporting businesses to protect their computer networks against cyber attacks. To manage analysts efficiently and effectively, SOC managers and stakeholders use Key Performance Indicators (KPIs) to evaluate their performance. However, existing literature suggests a lack of a systematic approach for assessing analysts' performance. Even though cyber security researchers advocate for research into this area, little effort has been made by researchers to address this gap. Drawing on the results of a Delphi panel with industry experts and the principles of the Analytic Hierarchy Process (AHP), this paper interrogates the problem and proposes a systematic weighted approach for measuring the performance of an analyst in a SOC. The proposed method, referred to as a SOC Analyst Assessment Method (SOC-AAM), was evaluated in two SOCs as a part of an experimental case study. The results of the empirical evaluation show that the SOC-AAM enables SOC managers and stakeholders to quantify and assess analysts' performance in a systematic manner. The SOC-AAM also provides a novel guideline for assessing the quality of incident analysis and the quality of incident reports. This study will be of interest to practitioners and cyber security researchers seeking to understand the operations of a SOC analyst.

1. Introduction

Security Operations Centres (SOCs) have had much increase in use and popularity in recent times and have become an active topic of research (Ahmad et al., 2021; Cho et al., 2020; Schlette et al., 2021; Vielberth et al., 2020). A SOC is a centralised unit inside or outside an organisation that helps businesses to defend their network against cyberattacks by monitoring and responding to security incidents (Achraf Chamkar et al., 2021; Majid and Ariffi, 2019). At the heart of a SOC's operations are cyber analysts (hereafter referred to as analysts) tasked with the responsibility of ensuring the smooth running of the SOC. It is the responsibility of an analyst to monitor, detect, analyse and report cyber threats and incidents (Kokulu et al., 2019; Smith, 2020). Analysts are expected to demonstrate high operational performance, because poor performance will negatively impact the overall efficiency of a SOC (Sundaramurthy et al., 2015).

To manage analysts effectively and efficiently, SOC managers and stakeholders draw on performance metrics and measures, also referred to as Key Performance Indicators (KPIs) (Onwubiko and Onwubiko, 2019) to evaluate analysts' performance (Onwubiko, 2015; Sundaramurthy et al., 2015; 2014). However, existing literature suggests that SOC managers and stakeholders face a challenge on how to evaluate the performance of analysts fairly and systematically (Achraf Chamkar et al., 2021; Andrade and Yoo, 2019; Sundaramurthy et al., 2015). Recent studies also point out that existing performance metrics and measures for evaluating the performance of an analyst are inadequate and problematic (Achraf Chamkar et al., 2021; Agyepong et al., 2019; Sundaramurthy et al., 2015; 2014; 2017). In the context of this work, the terms 'metric' and 'measure' are used interchangeably as they are closely linked and are often used synonymously (Ahmed, 2016; Jacques Houngbo and Toyigbé Hounsou, 2015). We use the term 'stakeholders' to describe other professionals in a SOC such as incident management manager, SOC team leaders and technical leads who are also interested in the performance of an analyst (Sundaramurthy et al., 2015).

Amongst the problems reported in the literature is that existing performance metrics for analysts do not consider several aspects of their work such as the quality of their analysis and

* Corresponding author.
E-mail addresses: agyeponge@cardiff.ac.uk (E. Agyepong), cherdantsevayv@cardiff.ac.uk (Y. Cherdantseva), reineckep@cardiff.ac.uk (P. Reinecke), burnapp@cardiff.ac.uk (P. Burnap).

https://doi.org/10.1016/j.cose.2022.102959

the handling of false positive security alerts (Agyepong et al., 2020b; Sundaramurthy et al., 2015). Furthermore, there is a concern that existing quantitative performance metrics fail to take into account the severity or priority of alerts processed by an analyst (Kokulu et al., 2019), even though researchers point out that analysts are expected to analyse security alerts according to alert priority (Onwubiko and Ouazzane, 2019c; Shah et al., 2018). The problem of ignoring alert priority, and simply measuring analyst performance based on the number of incidents actioned regardless of their severity, is that some analysts may opt to action a large number of easy, benign or low priority incidents, thereby scoring high on such a metric (Sundaramurthy et al., 2017). Prior research also highlights that existing metrics are narrow in focus and discrete and, as such, do not present the entire picture of an analyst's efforts and performance within a SOC (Sundaramurthy et al., 2015). Some researchers also assert that SOC managers usually focus on quantitative metrics with little attention on qualitative metrics such as quality of analysis when measuring the performance of analysts (Achraf Chamkar et al., 2021). In addition, studies suggest that the current lack of a systematic approach for evaluating the performance of analysts frustrates both analysts and SOC managers (Sundaramurthy et al., 2015; 2017). Despite the problems mentioned above, there has been little effort from cyber security researchers to improve evaluation methods for analysts.

The main contribution of this work is a method for evaluating the performance of a SOC analyst in a comprehensive and systematic way accounting for the level of importance of each function. The proposed method includes a novel guideline for assessing the quality of incident analysis conducted by analysts and the quality of their incident reports. This guideline will be helpful to both experienced and novice analysts who study suggest suffer from the complexities of security incident analysis tasks (Zhong et al., 2018). We refer to the proposed method as the Security Operations Centre Analysts Assessment Method (SOC-AAM).

This work builds on our previous study that identified the main functions of analysts in a SOC and the criteria that could be used to measure their performance systematically (Agyepong et al., 2020b). In this work, we draw on the results of a Delphi panel of SOC experts and the principles of the Analytic Hierarchy Process (AHP) to propose a weighted approach for measuring the performance of an analyst. We tested and evaluated the proposed method in a case study at two SOCs. The evaluation results show that the SOC-AAM enables SOC managers to aggregate and quantify the performance of an analyst in a systematic manner. The results also reveal that the SOC-AAM offers a useful, easy-to-use and comprehensive approach for evaluating an analyst's performance.

The remainder of the paper is organised as follows: Section 2 discusses related work, focusing on studies that examine performance metrics for analysts. In Section 3, we present a discussion on the operations of SOC analysts from a theoretical perspective. Section 4 presents the methodology used for this study, explaining both the Delphi technique and the AHP methods. Section 5 presents the results of the Delphi panel. Section 6 presents the proposed method. Section 7 presents the results from the testing and evaluation of the weighted approach. Section 8 presents a discussion and research implications. Section 9 presents the conclusions and future work.

2. Related work

Cyber security researchers have suggested various KPIs for evaluating the performance of analysts (Agyepong et al., 2019; Kokulu et al., 2019; Onwubiko, 2015; Sundaramurthy et al., 2015; 2014; 2017). KPIs are measures for assessing performance (Kaplan, 2009; Onwubiko and Onwubiko, 2019). However, studies suggest that SOC managers and analysts could benefit from an alternative approach to evaluating an analyst's performance (Sundaramurthy et al., 2015; 2014). In a previous work (Agyepong et al., 2020b), we conducted an empirical case study to understand the real work of a SOC analyst and proposed a framework that was validated by SOC experts as a useful framework that provides the foundation for developing an approach for capturing the holistic performance of an analyst. This paper builds on the findings of our previous work and proposes a method for evaluating an analyst's performance.

Sundaramurthy et al. (2014) visited three SOCs to identify, amongst other things, metrics for evaluating the performance of an analyst and found that while some SOCs use the number of incidents processed by an analyst at the end of their shift to assess their performance, other SOCs measure analysts' performance based on the time it takes to create a ticket. Their study acknowledged that there are problems with both metrics. For example, whereas the latter fails to recognise that some security incidents are more complex than others and will naturally require more time, a performance metric based on the number of incidents raised, as explained by Kokulu et al. (2019), does not consider the alert priority or severity. Thus, there will be no difference between analysts who consistently work on critical severity incidents and those who choose to work on low priority incidents.

A subsequent study by Sundaramurthy et al. (2015) that sought to investigate a burnout phenomenon amongst analysts found that a major challenge faced by SOCs is how to evaluate the performance of analysts in an objective and consistent manner. Sundaramurthy et al. (2015) noted that the existing evaluation methods fail to fully capture the efforts of an analyst, leading to frustration and dissatisfaction amongst analysts. They report that some SOCs based analysts' performance on the time they spend creating a ticket. They noted that analysts lament because tasks such as dealing with false-positives and tuning out of false-positive alerts, are often not recognised when it comes to performance assessment.

Onwubiko (2015) discusses a number of metrics that can be used by SOC managers to measure the performance of analysts. Amongst them are the number of incidents detected in a certain period, the number of false positives and true positives detected over a rolling period. However, these performance metrics have similar problems as stated above.

Achraf Chamkar et al. (2021) and Kokulu et al. (2019) also present performance metrics such as the number of incidents raised, the number of alerts analysed by an analyst during their shift, mean time to detect (MTTD) and mean time to respond (MTTR) to an incident. However, analysts see time-based measures such as MTTD and MTTR as misleading when used to evaluate their performance because there are often issues outside their control (such as, for example, reliance on third parties for collaborative evidence) (Achraf Chamkar et al., 2021; Agyepong et al., 2020b).

Shah et al. (2018) propose evaluating the performance of an analyst based on the number of analysed/unanalysed alerts actioned by an analyst operating an Intrusion Detection System (IDS) sensor. Their approach, however, does not account for other activities performed by an analyst.

The work presented in this paper takes a different approach to how an analyst's performance can be measured. We propose a weighted approach for evaluating an analyst performance using multiple criteria based on the most common and significant aspect of analysts work identified in previous work (Agyepong et al., 2020b). We also presents a guideline for assessing the analysis and incident report produced by analysts.

3. Key functions of a SOC analyst

Analysts play a vital role in the operations of a SOC and the delivery of a SOC's services (Aung et al., 2020; Axon et al., 2017).

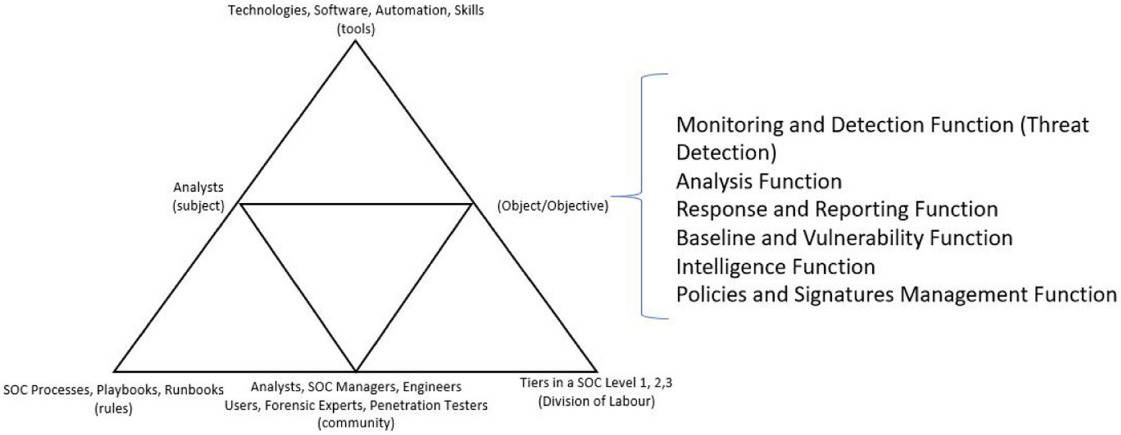
Technologies, Software, Automation, Skills
(tools)
Analysts
(subject)
(Object/Objective)
Monitoring and Detection Function (Threat Detection)
Analysis Function
Response and Reporting Function
Baseline and Vulnerability Function
Intelligence Function
Policies and Signatures Management Function
SOC Processes, Playbooks, Runbooks
(rules)
Analysts, SOC Managers, Engineers
Users, Forensic Experts, Penetration Testers
(community)
Tiers in a SOC Level 1, 2,3
(Division of Labour)

Fig. 1. Activity Theory in SOCs extended from Sundaramurthy et al. (2016).

From a theoretical perspective, the activities and operations of analysts can be understood using the Activity Theory (AT) (Sundaramurthy et al., 2016). The AT, which was first postulated by Leontiev and Vygotsky, and subsequently extended by Engeström (2015), can be used to model any organised human activity.

The underlying assumption of the AT is that humans are collective beings and that their actions are goal-directed or objective-directed (Engeström et al., 1999). According to the AT, without an objective, there is no meaning to any planned human activity (Sundaramurthy et al., 2016). The AT stresses that humans do not act in isolation but within communities (Engeström, 2015). This theory is very much evident in the operations of analysts and how they engage with other members of the team to execute missions and realise key objectives successfully. To achieve their objectives, they must obey the rules that govern the activities of analysts in a SOC. Rules can be in the form of processes such as Standard Operating Procedures (SOPs), playbooks and runbooks (Sundaramurthy et al., 2014). Analysts also rely on tools such as firewalls, Security Information and Event Manager (SIEM) and Intrusion Detection and Prevention Systems (IDPSs) to achieve their objectives. They also draw on the idea of division of labour through the operations of different tiers of analysts (Level 1, 2, and 3) to achieve their objectives Kokulu et al. (2019); Sundaramurthy et al. (2014, 2016). Although some SOCs do not use a three-tier architecture and instead rely on their analysts to possess the necessary analytic abilities to undertake their task (Kokulu et al., 2019). Analysts also engage with professionals such as SOC engineers, incident handlers, penetration testers and forensic specialists in the course of their operations within a SOC (Agyepong et al., 2020b). It is important to mention that not all SOCs operate using the Tier structure. In a in non-hierarchical SOC, all the analysts are expected to have similar skill-sets to address security incidents (Kokulu et al., 2019).

Although Sundaramurthy et al. (2016) provide an organised account of the activities of analysts within a SOC by drawing on AT, their discussion only focuses on the threat detection function (the monitoring and detection function) by analysts. They do not thoroughly discuss other salient objectives pursued by analysts that are relevant when seeking to assess their holistic performance. For example, they do not discuss or comment on key analysts' objectives such as finding and fixing vulnerabilities (Agyepong et al., 2020b; Kokulu et al., 2019). Likewise, they also do not discuss objectives such as the baseline and vulnerability management function that are usually performed by analysts (Agyepong et al., 2020a; Schinagl et al., 2015). A revised version of the model suggested by Sundaramurthy et al. is presented in Fig. 1 to illustrate the operations of analysts and the full range of objectives expected of them.

The identification and appreciation of analysts' objectives, also referred to as analysts' functions in this study, are crucial if one wants to design or establish a systematic way of capturing analysts' holistic performance. These functions can be used as a set of criteria for evaluating analysts' performance (Agyepong et al., 2020b). Moreover, an effective evaluation method, as explained by Islam and bin Mohd Rasad needs to have a set of well-defined criteria upon which the evaluation is based (Islam and bin Mohd Rasad, 2006). O'Connell and Choong (2008) explain that performance metrics must focus on an analyst real-life workplace needs and experience. However, this can be a problematic issue because no two SOCs are the same in terms of the functions that they offer; analysts' functions vary from one SOC to another (Goodall et al., 2004; Onwubiko, 2015; Schinagl et al., 2015). With this idea in mind, in this study we designed a performance evaluation system, based on the most common and significant functions of analysts.

The functions of analysts are shown in Fig. 1. These functions were identified in previous work and validated by a group of SOC analysts and managers as the core functions of an analyst that can be used as the basis for measuring an analyst's overall performance (Agyepong et al., 2020b). Existing literature also identifies these functions as core functions of a SOC (Onwubiko, 2015; Schinagl et al., 2015). Table 1 summarises the main functions expected of an analyst and a description of each function.

A number of qualitative and quantitative KPIs were also identified as useful metrics for measuring the performance of an analysts under each function. However, on their own, the different functions and KPIs are discrete and as such do not provide an overall insight into the performance of an analyst if used in a disconnected manner. The intention of this study is, therefore, to find a systematic way of consolidating the functions expected of an analyst and the associated KPIs for each function to derive the overall performance of an analyst. It is important to highlight that time-based KPIs such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Triage (MTTT), Mean Time to Fix Vulnerability (MTTFV) and Mean Time to Mitigate (MTTM) (Achraf Chamkar et al., 2021; Agyepong et al., 2020b) are not used in the evaluation method proposed in this study for the reasons discussed under Section 2.

4. Research methodology

In order to propose a new approach for measuring the performance of an analyst, this study adopts a practical research method-

Table 1
The main functions of a SOC Analyst (Agyepong et al., 2020b).

Analysts' Functions	Description of Activities
Monitoring and Detection Function	• Real-time event monitoring of an organisation's network traffic, systems, processes and activities using security tools such as a SIEM, an IDS or IPS to identify malicious activities. • Monitor security systems such as firewalls to detect policy violation, privilege user activities, security breaches or any unusual activity on the network. • Identification of false positives and false negatives from sensors and tuning them out to decrease the load on sensors and analysts. • Deep packet inspection and alert triage.
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 to establish whether an activity poses a threat to an organisation. • Drawing on historical logs to confirm trends and patterns. • Conducting root cause analysis and creating script queries to investigate logs.
Baseline and Vulnerability Function	• Vulnerability scans. • Applying Patches to fix vulnerabilities. • Hardening systems, closing unused ports, disabling unused services. • Ensuring that systems are patched to the correct level and that all systems running unsupported operating systems are identified.
Intelligence Function	• Identify threat actors that may pose a danger to an organisation. • Exchanging threat information with various internal and external parties. • Correlate information on multiple 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.
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 incident reports.
Policies and Signature Management	• Writing and tuning correlation rules. • Signatures and rules modification to remove false positives. • Modification to customised Signatures and content rules.

ology that engages with industry experts. The Delphi technique (Turoff and Linstone, 2018) and the Analytic Hierarchy Process (AHP) (Saaty, 2008), were used during the engagement with the experts. Even though these two methods have been combined and used in several studies (Arof, 2015; Taleai and Mansourian, 2008), to the best of our knowledge, there is no existing work that integrates both approaches in the context of assessing a SOC analyst's performance.

To assess the efficacy of the proposed method, we use the Method Adoption Model (MAM). The MAM is based on the Method Evaluation Model (MEM) - a theoretical framework for validating IS design methods. However, as explained by Paz et al. (2015) the MEM has general aspects of evaluation that can be applied to any kind of design method. According to the MEM, the success of a design method is reflected in its adoption into practice. Moody (2003) posits that the acceptability and use of a method in practice (which is the ultimate measure of its success) is driven by a set of perceptions and intentions. Only methods that are considered to be useful and easy-to-use will motivate practitioners to use it again in the future. The intention to use a particular method leads to its 'Actual Usage' in practice, which ultimately signifies the success of that method (Paz et al., 2015). On the contrary, if practitioners do not have a good perception of a method, they are not likely to adopt or use it. We validated the proposed method in two SOCs using this evaluation strategy. Section 7 discusses the evaluation process in greater detail.

4.1. The Delphi method

The Delphi method is a widely used technique for gathering data from a group of experts on a topic within their domain of expertise in a structured group communication (Turoff and Linstone, 2018). It is useful in situations where no standard criteria exist for evaluation, as in the case of the SOC analyst performance (Paintsil, 2012). However, the Delphi method has some drawbacks one of which is that it can be a laborious and time-consuming method because of the multiple rounds and associated feedback process for each round (Turoff and Linstone, 2018). A typical Delphi process usually involves a minimum of two rounds (Arof, 2015).

In this study, the Delphi method was used to solicit the opinion of SOC experts on the weights that should be assigned to the analysts' functions and KPIs that can be used for measuring the performance of analysts. These functions and KPIs are also referred to as assessment 'criteria' and 'subcriteria', respectively, to align the functions and associated KPIs to the AHP terminology as part of this study. As mentioned earlier, the analyst's functions (criteria) and KPIs (subcriteria) were identified as part of our earlier work with SOC experts (Agyepong et al., 2020b). Identification of the criteria and the subcriteria for the evaluation is an integral part of the AHP decision-making process (Saaty, 1990) discussed in the next section. In addition, we used the Delphi technique to solicit experts' opinions on key indicators that can be used to assess the quality of an analyst's analysis and the quality of their report.

In the literature, different Delphi methods exist, giving researchers a choice on the specific Delphi technique to use, depending on what they seek to uncover (Arof, 2015; Ogbeifun et al., 2016). The decision-making Delphi is adopted in this work as it follows a structured approach that allows experts to create a future reality, based on the choices they make (Arof, 2015). Arof (2015) explains that the decision-making Delphi option is similar to the classical Delphi method because they follow similar steps. These steps are summarised in Gan et al. (2015) as follows: (1) Design the questionnaire and identify the Delphi panel; (2) Undertake the first round of the Delphi survey with the expert panel; (3) Synthesise the opinion provided by the experts from the first round and provide that feedback to all the members on the panel; (4) Request that each member of the panel reconsider the decision, based on the findings from the experts from the first round; (5) Synthesise expert opinion from the second round and reach a consensus; (6) Repeat steps 3 to 4 (if necessary) until a uniform result is achieved on the topic. These six steps were followed in conducting our Delphi exercise.

We began the Delphi study by contacting the SOC experts who took part in our earlier work that identified the criteria that can be used to evaluate the performance of analysts. On the recommendation from the recruited participants, we also contacted other SOC experts who did not take part in our previous study. As explained by Akins et al. (2005) participants for a Delphi study are not randomly selected but rather they are purposively selected as they have the knowledge and insight on the topic under study. We sent an email to the participants, explaining the objective of the research and requested their participation. In total, 11 (eleven) SOC experts initially agreed to take part in the study. However, only 8 (eight) of them completed and returned their questionnaires. With regard to our study sample size, although there is no consensus on the minimum number of participants for a Delphi study, we noted that some scholars point out that the panel size for a Delphi study can be as small as three participants (Arof, 2015; Ogbeifun et al., 2016; Turoff and Linstone, 2018). The panel consisted of SOC managers and analysts from the UK Defence sector, finance sector, the airline industry, the automobile industry and telecommunication.

4.2. The Analytic Hierarchy Process Method

The Analytic Hierarchy Process (AHP) is a mathematical model that facilities multi-criteria decision-making involving both qualitative and quantitative criteria at an individual or group level (Saaty, 2008; 1980). Since its inception, the AHP has been used in several fields, including computer science and information systems (Badie and Lashkari, 2012; Benítez et al., 2011; Costa and Santos, 2017; Fahmy, 2001; Siregar and Siregar, 2018). The AHP breaks a complex problem into modular parts; arranges these parts into a hierarchy; assigns numerical values to the criteria/elements in the hierarchy by making a pairwise comparison on the relative importance of each criterion, and synthesises the judgement to establish priorities (also known as weights) (Odu, 2019; Saaty, 2008). Once the weights are obtained, a consistency check is applied to ensure that the judgements are not made arbitrarily (Odu, 2019), reducing bias in the pairwise comparisons process. If the judgements are found to be inconsistent, the judgement needs to be re-evaluated (Benítez et al., 2011).

Islam and bin Mohd Rasad (2006) outlined four steps to using the AHP to evaluate the performance, which are:

i. Identify the criteria, subcriteria and employees to be evaluated and construct the AHP model/hierarchy;
ii. Construct an $n \times n$ pairwise comparison matrix for the criteria. Calculate the weights of the decision criteria by computing the normalised principal eigenvector of the matrix (Odu, 2019). This vector gives the weights of the criteria (Saaty, 2003; Singh Sidhu et al., 2020; Vargas, 2010). Construct a pairwise comparison for the subcriteria and calculate the weights in a similar manner. The weights of the subcriteria are multiplied by their respective parent criterion;
iii. Divide each subcriterion into intensities or grades such as high, medium, and low. The intensity allows one to determine the quality of an alternative for that criterion (Saaty, 2008). Priorities are assigned to the intensities by conducting a pairwise comparison. The priorities of the intensities are multiplied by the weight of their parent subcriterion;
iv. Finally, take each employee and measure their performance intensity under each subcriterion, then add the global priorities of the intensities for the employee. Repeat the process for all the employees.

The approach used in this study is similar to the steps described above; however, in our work, step (iii) is replaced with the inherent intensities of the KPIs: the individual KPIs achieved by an analyst under step (ii) are also used as the distinguishing factor instead of creating a new set of intensities. As explained by Saaty (Saaty, 2008, p.136), the purpose of intensities is to distinguish the quality of an alternative for that criterion. Since many of the KPIs used as the subcriteria (see Fig. 2) are already serving as a distinguishing factor (for example, incidents processed by analysts are categorised as high incidents, medium incidents and low incidents (Onwubiko and Ouazzane, 2019c; Shah et al., 2018)), we opine that there is no need for additional intensities to be created. We do not use intensities under the intelligence function, the policies and signatures management function, and the baseline and vulnerability management function because the KPIs under these functions are deemed sufficient to capture the performance of an analyst, as we discovered during our fieldwork with SOC experts (Agyepong et al., 2020b). This strategy is similar to the work of Vargas (2010), who did not use intensities. In step (iv), each analyst is measured against each KPI, and the total of the KPIs is used to determine their overall score.

Figure 2 depicts the architecture of the AHP hierarchical model used in this study. The first level of the hierarchy represents the goal, which is to measure the overall performance of an analyst. The second level of the hierarchy represents the main functions of an analyst which are also used as the main criteria used for the evaluation process in this work. The functions of analysts were deduced from the empirical interview data collected from SOC experts (Agyepong et al., 2020b) and a thorough analysis of existing literature (Goodall et al., 2004; Onwubiko, 2015; Schinagl et al., 2015). The third level of the hierarchy represents the subcriteria for each respective main criteria. The KPIs under each function are used as the subcriteria. The final level represents the analysts who are evaluated one at a time against the criteria and subcriteria defined above. The word *'alternatives'* is often used in the AHP hierarchy to denote the final level.

4.2.1. Applying the AHP to derive the criteria weights

Having modelled the AHP hierarchy, a pairwise comparison matrix A is constructed and used to compute the weights for the criteria and subcriteria. The matrix A is an $n \times n$ real matrix, where n is the number of evaluation criteria or subcriteria being considered. Let a_{ij} be a pairwise comparison that the decision-maker makes between two criteria i and j. Each entry a_{ij} of the matrix A represents the importance of the ith criterion relative to the jth criterion. Note that, a_{ij} denotes the entry in the ith row and the jth column of matrix A. If $a_{ij} > 1$, then the ith criterion is more important than the jth criterion, whereas if $a_{ij} < 1$, then the ith criterion is less important than the jth criterion. If the two criteria have the same importance, then the entry a_{ij} will be equal to 1 (Saaty, 2008). In AHP, the entries a_{ij} and a_{ji} satisfy the constraint: $a_{ij} \cdot a_{ji} = 1$ and $a_{ii} = 1$ for all i. If $a_{ij} = 1$, it means that the decision-maker regards element i and j as equally important.

The relative importance between two criteria is measured according to the numerical scale of 1 to 9, shown in Table 2.

Once the matrix A has been constructed, the priority vector (or weights) for the criteria can be calculated (Islam and bin Mohd Rasad, 2006). The process for deducing the weights starts by deriving from the matrix A a normalised pairwise comparison matrix (A_{norm}) by making the sum of each column equal to 1 (Odu, 2019). Eq. 1 is used for the computation. Each entry $\bar{a}_{ij}$ of the matrix A_{norm} is computed, using Eq. 1 (Ishizaka and Labib, 2011).

$$\bar{a}_{ij} = \frac{a_{ij}}{\sum\limits_{i=1}^{n} a_{ij}} \tag{1}$$

Finally, the criteria weight vector (w) is calculated by averaging the entries on each row of A_{norm} using Eq. 2 (Ishizaka and Labib,

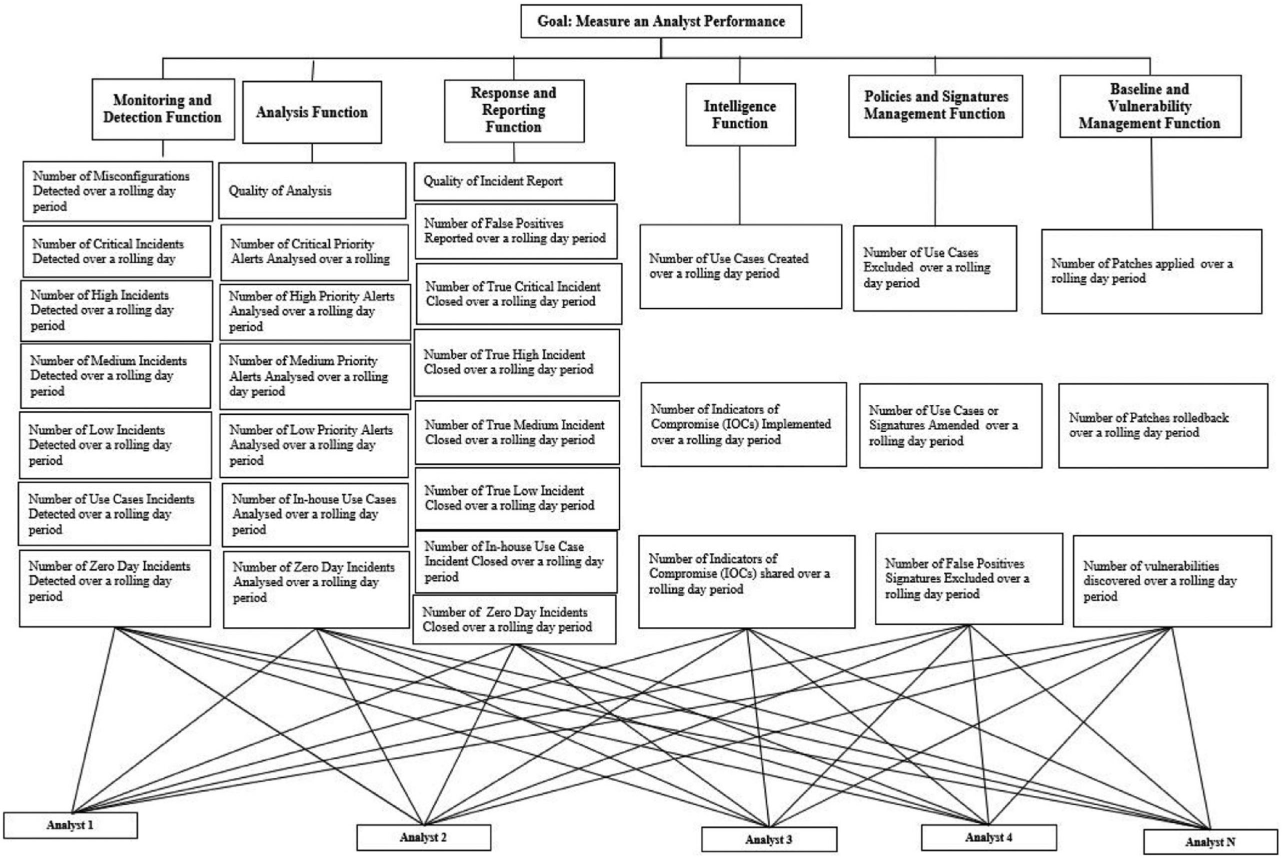
Goal: Measure an Analyst Performance
Monitoring and Detection Function
Analysis Function
Response and Reporting Function
Intelligence Function
Policies and Signatures Management Function
Baseline and Vulnerability Management Function
Number of Misconfigurations Detected over a rolling day period
Number of Critical Incidents Detected over a rolling day
Number of High Incidents Detected over a rolling day period
Number of Medium Incidents Detected over a rolling day period
Number of Low Incidents Detected over a rolling day period
Number of Use Cases Incidents Detected over a rolling day period
Number of Zero Day Incidents Detected over a rolling day period
Quality of Analysis
Number of Critical Priority Alerts Analysed over a rolling
Number of High Priority Alerts Analysed over a rolling day period
Number of Medium Priority Alerts Analysed over a rolling day period
Number of Low Priority Alerts Analysed over a rolling day period
Number of In-house Use Cases Analysed over a rolling day period
Number of Zero Day Incidents Analysed over a rolling day period
Quality of Incident Report
Number of False Positives Reported over a rolling day period
Number of True Critical Incident Closed over a rolling day period
Number of True High Incident Closed over a rolling day period
Number of True Medium Incident Closed over a rolling day period
Number of True Low Incident Closed over a rolling day period
Number of In-house Use Case Incident Closed over a rolling day period
Number of Zero Day Incidents Closed over a rolling day period
Number of Use Cases Created over a rolling day period
Number of Indicators of Compromise (IOCs) Implemented over a rolling day period
Number of Indicators of Compromise (IOCs) shared over a rolling day period
Number of Use Cases Excluded over a rolling day period
Number of Use Cases or Signatures Amended over a rolling day period
Number of False Positives Signatures Excluded over a rolling day period
Number of Patches applied over a rolling day period
Number of Patches rolledback over a rolling day period
Number of vulnerabilities discovered over a rolling day period
Analyst 1
Analyst 2
Analyst 3
Analyst 4
Analyst N

Fig. 2. SOC Analysts' Assessment Criteria.

Table 2
Saaty's Scale of Relative Importance (Saaty, 2008).

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

2011; Odu, 2019).

$$w_i = \frac{\sum_{j=1}^{n} \overline{a}_{ij}}{n} \tag{2}$$

4.2.2. Checking the consistency

The consistency of the choices made by the decision-maker for a comparison matrix can be checked by calculating the consistency ratio (CR). (CR) can be calculated using Eq. 3 Saaty (2008).

$$CR = \frac{CI}{RI} \tag{3}$$

In Eq. 3, RI denotes a Random Index. In a randomly generated matrix, the values are entered randomly and expected to be inconsistent (Saaty, 2008). Table 3 shows the values for RI (Saaty, 2008).

Also, the CI in Eq. 3 is calculated using Eq. 4, where ($\lambda_{\max}$) represents the maximum eigenvalue of the decision matrix A and n is the number of compared criteria Saaty (2008). The comparison matrix A is absolutely consistent if $\lambda_{\max} = n$; otherwise as explained by Saaty (2008), the difference $\lambda_{\max}$ n will be a measure of inconsistency in the decision matrix.

If A is absolutely consistent then $\lambda_{\max} = n$ (Vargas, 2010). If the CR of the decision matrix is less than 0.1, then, the judgement is acceptable and can therefore be used (Odu, 2019).

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{4}$$

Having done the calculations for the main criteria, a similar calculation is repeated for all subcriteria. Once the local priorities of the subcriteria are calculated, they can then be aggregated to get the final priorities (Vargas, 2010).

As a part of the integrated Delphi-AHP approach, the participants were given a questionnaire for the pairwise comparison. The questionnaire was devised in a spreadsheet and was submitted to the members of the Delphi panel via email, a strategy which is similar to the suggestion by Gordon (2011). To aggregate the results from the panel (group), a number of techniques can be used (Ishizaka and Labib, 2011). Saaty (2008, p. 273) suggests that consensus can be reached by taking the geometric mean of the in-

Table 3
The consistency indices for a randomly generated matrix.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R1	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.52	1.54	1.56	1.58	1.59

dividual responses or by voting on the preferred judgement for each pairwise comparison. This position is supported by scholars such as Ishizaka and Labib (2011). In this study, the geometric mean of the pairwise judgements from the participants was used in favour of voting as it was not possible to get all participants together to vote. The geometric mean values from the experts were used to construct a pairwise comparison table in a manner satisfies the reciprocal relation in comparing the elements (De Felice and Petrillo, 2013).

It is important to point out that, the participants were provided with a recorded video demonstrating the AHP pairwise comparison exercise and guidance on how to complete the accompanying excel spreadsheet for their individual AHP judgements. The purpose of the video was to familiarise the participants with the AHP concept. The excel spreadsheet was also designed to check the consistency of the pairwise comparison and report back to the participant if their judgement was inconsistent. This enables the participants to adjust to their pairwise comparison until they were consistent.

5. Study results

This section presents the results of the Delphi Study and the aggregated outcome of each round.

5.1. Round 1 - Decisions matrices

We analysed individual responses from Round 1 to ensure that it satisfied the rule of reciprocity, transitivity and was aligned to the AHP consistency index (De Felice and Petrillo, 2013). The rule of reciprocity dictate that when a judgement a_{ij} is elicited, a_{ji} will also be recorded as the reciprocal value in the comparison matrix. On transitivity, we explain that this relates to the judgement choices made by the decision maker. For example, if a decision maker prefers summer twice as much as spring and spring twice as much as winter, in mathematical terms,the preference of summer to winter would be 4. If the decision-maker assigns any other value, there would be a certain level of inconsistency in the judgement (Saaty, 2008). The geometric mean of the values suggested by the participants for the main criteria was then used to construct the group's comparison matrix, shown in - Appendix A. We then checked the consistency index of the group's decision. The resultant weights for each of the main functions along with the *CR* are shown in Appendix A, Table 8.

We applied a similar approach to derive the weights for the subcriteria and computed their respective *CR*. The results of the weights for all the criteria and subcriteria are shown in Appendix A - Tables 9, 10, 11, 12, 13, 14. The analysis of the data from the panel in Round 1 shows that the group's aggregated result was below the AHP consistent ratio of < 0.1. The findings from Round 1, which met the AHP standard, led us to adopt a two-round Delphi approach (Arof, 2015).

5.2. Round 2 - Final ranking and weights

The objective of Round 2 was to establish whether the experts agreed with the group consensus achieved in Round 1, or whether any of the participants wanted to modify the values from the group judgement. Round 2 gave the experts the opportunity to make any changes or to recommend further improvement of the results from Round 1.

The outcome at the end of Round 2 revealed some interesting results in that the participants were satisfied with the weights that had been assigned to the different tasks. As a result, no changes were made to the weights deduced from the group consensus in Round 1. Hence, the weights deduced from the group's decision are proposed as the final weights for measuring the performance of analysts.

The weights for the criteria and subcriteria from the two rounds were synthesised to yield a set of overall weights (also known as the "global weights"), by multiplying the weight of each criterion by the respective weights of their subcriteria (Vargas, 2010). The output of the calculation is shown in Appendix B, Table 15.

In addition to the weight assignment, the experts were also invited to suggest "indicators" for assessing the quality of an analyst's report and the quality of their analysis as part of the Delphi study. The word "indicators" in this study denotes guidelines for assessing the quality of an analyst's incident analysis/report. Related publications point out that incident analysis and report must address 'who' (attacker/malicious person), 'what' (indicators of compromise/actions done), 'where' (from what IP address), 'when' (timestamp), 'why' (the risk), 'how' (method of detection) and provide recommendations on the actions taken to address the identified incident. Using an insight from the existing work (D'Amico et al., 2005; Miloslavskaya, 2018; Mutemwa et al., 2018; Zhong et al., 2016), we devised a table and listed some indicators that can serve as a guideline for assessing the quality of an analyst's report. The experts were requested to review and add to a list of indicators.

Following the two rounds of the Delphi study, the indicators identified in Table 4 were reported by the participants as the most important areas that must be reported by analysts as part of quality analysis and in their reports. These indicators can help assess the quality of an incident report written by an analyst.

5.3. Reflection on the Delphi-AHP exercise

Although there was a group consensus on the weights for the different functions, it is important to highlight that there were some differences at an individual level in how the participants perceived the importance of functions, which was reflected in the AHP values that were assigned. In fact, the differences in opinions, which were reflected in the responses to the questionnaire, confirm the assertion made by Goodall et al. (2004), that different SOCs conceptualise the operations of a SOC differently. It is, therefore, possible that our respondents' opinions were influenced by the importance they attached to the functions in their local SOCs. Another notable observation from the AHP questionnaire returned by that participants was that some of the panel members assigned an AHP value of 1 to many of the functions, which may have facilitated the achievement of a group consensus that was consistent with the AHP *CR* of < 0.1.

Despite the individual differences in opinion observed in the pairwise comparison values, the inference can be made that the participants collectively tended to agree that the monitoring and detection function, the analysis function and the response and reporting functions were the most important. As such, these functions were assigned the highest weights, confirming the importance of these three functions as reported by previous SOC researchers (Agyepong et al., 2020b; Jacobs et al., 2013; Onwubiko, 2015).

Table 4
Quality of Analysis and Quality Report Criteria.

ANALYSTS NEED TO IDENTIFY & REPORT ON THE FOLLOWING (IF AVAILABLE) TO ACHIEVE QUALITY ANALYSIS & A QUALITY REPORT.						
01 - WHO	02 - WHERE	03 - WHEN	04 - WHAT	05 - WHY	06 - HOW	07 - RECOMMENDATION
Who are the potential attackers/adversaries?	Where is the attacker or adversary targeting or likely to target and exploit?	When was the attack or incident first noticed?	What does the attacker already know? What capability do the attacker have?	Why is this incident of interest?	How was the potential attack discovered?	Recommendation for addressing the Incident.
• Attack Path (External threat or Insiders?) • Source IP Address/Attacker IP Address • Source Port/Service • Source MAC Address • Attacker Username (if internal) • Attacker Host Name • Attacker User Agent (if applicable)	• Impacted Host/Application • Destination IP Address • Destination Port/Service • Destination MAC Address • Location of Detection	• Date and Time of Detection including time zone • Reporting Device • Detection time • Manager Receipt Time	• Name of Alert/Incident/Trigger • File/Email/URL/Domain Name • Asset Name • User Account • IPS Signature/Use Case • Event ID/Type/OS • Breach Type • Incident Severity/Classification • File Hash • Indicator of Compromise • Vulnerabilities of the target system (with or without public exploits)	• Risk • Context and geographical Information and threat description • System criticality • Potential Impact	• Method of Detection • Mitigation Factors • Playbook used (Enter playbook used for incident (if any) (Phishing Playbook, Enrichment Playbook etc)	• Containment Strategy • Mitigation Strategy • Any contact details (E.g. Email, Phone number, Office) - for further investigation • Creation of a new use case or signature (if required) • Eradication and remediation • Return to business operations

6. Security Operations Centre Analysts' Assessment Method (SOC-AAM)

In the SOC-AAM, we assign the final weights deduced from the Delphi-AHP study to the functions of an analyst (see Appendix C - Table 16). The SOC-AAM contains six main analyst's functions and 31 KPIs. These six functions and associated KPIs are shown in the first column of the SOC-AAM. The second column of the SOC-AAM shows the weight for each function and for each KPI. The third column (labelled - "KPI Score") is reserved for the KPI score achieved by an analyst over the assessment period. An assessor or evaluator must enter the value(s) for the third column during the evaluation process. The fourth column (Analyst's Score Per Activity) represents the aggregated score per each function. The fifth column (labelled - Team's Total KPI) is reserved for the KPI score achieved by the entire team over the assessment period. The final column (Team's Overall Score) represents the team's aggregated score per each function. The rows labelled "Analyst's Overall Score" and "Team's Overall Score", shown at the bottom of the SOC-AAM, represents the aggregated score for an analyst and that of the team respectively, once the score(s) for each KPI have been entered by an evaluator. This process is further described below. The performance of the analyst is calculated in percentage terms, considering the overall team's performance in the assessment period. This is to help track and compare the performance of the team and each individual analyst over time.

The steps required to use the SOC-AAM as an evaluation tool are detailed below. The process is facilitated by an Excel spreadsheet that automates all calculations. The output of the SOC-AAM is an aggregation of the KPI scores for a set of SOC analyst's functions. Under each function, the number of achieved KPI(s) for the function is submitted. If there are no scores for a particular function, that should be left blank. For example, the number of incidents closed will be reported under the Response and Reporting function.

The SOC-AAM contains two special KPIs (the quality of analysis and the quality of incident report) that must be scored by only a SOC manager or the technical lead, as part of the evaluation process. These two KPIs are important because they are among the top three largest weights in the SOC-AAM and are based on the subjective judgement of the evaluator. As a part of the evaluation process, a SOC manager needs to review a randomly selected report written by an analyst during an assessment period and assign a score between 1 to 7 (where 1 is the lowest and 7 is the highest), depending on how many of the seven quality indicators the analyst has addressed in the report (see Fig. 4). In our previous work, we found that the quality of analysis is often reflected in the report written by an analyst (Agyepong et al., 2020b). Therefore, the manager could assign the same score to both the quality of analysis and the quality of the report. Alternatively, she/he could choose to assign a different score for quality of analysis up to a maximum of 7. However, this does not suggest that the quality of analysis is the same as the quality of report, since the research participants assigned different weights for the quality of analysis and the quality of the report.

The steps for evaluating analysts' performance are outlined below:

- Step 1: The evaluator enters the total number of analysts in the team into the SOC-AAM tool. This will calculate the maximum team score for the quality of analysis and the quality of their report. (Note: Each analyst can achieve only a maximum score of 7 for the quality of their analysis and 7 for the quality of their report, based on the seven indicators as stated earlier; the overall team score is, therefore 7, multiplied by the number of analysts for each of the two functions);
- Step 2: If an analyst has written a report over the assessment period, the SOC manager or the technical lead must review the report and assign a score between 1 and 7 for the quality of report. The manager would also assign a score for the quality of analysis as explained above;

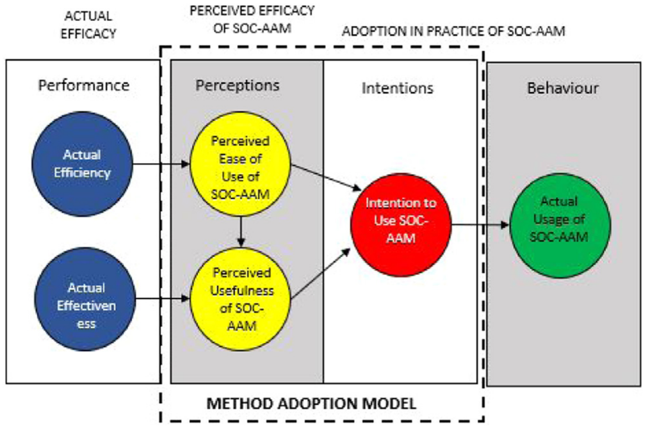

Fig. 3. The Method Evaluation Model (Moody, 2003; Paz et al., 2015).

- Step 3: The evaluator must enter the scores for the remaining functions. Once the evaluator has entered all the scores, the SOC-AAM tool will automatically calculate an analyst's overall performance score; and
- Step 4: To allow a comparative assessment of an analyst's performance against their peers, the team's total scores for each function must be entered for the evaluation period. Once completed, the score for individual analysts would be displayed as a percentage to reflect their individual contribution to the overall team's effort for a reporting period.

7. Empirical evaluation of the SOC-AAM

The Method Adoption Model (MAM) (Paz et al., 2015) was used to evaluate the efficacy of the SOC-AAM. As mentioned in Section 4, the MAM is derived from the Method Evaluation Model (MEM) (Moody, 2003), a theoretical framework for validating design methods.

The MEM consists of six constructs whose relationship are shown in Fig. 3. The definitions for the MEM constructs which we adopted (Moody, 2003; Paz et al., 2015; Recker, 2008) are as follows:

- Actual Efficiency: refers to the effort required to apply a method;
- Actual Effectiveness: denotes the degree to which a method achieves its objective;
- Perceived Ease of Use (PEOU): refers to the degree to which a person believes that using a method would be free of effort;
- Perceived Usefulness (PU): denotes the degree to which a person believes that a particular method will be effective in achieving its intended objective;
- Intention to Use (ItU): denotes the extent to which a person intends to use a particular method; and
- Actual Usage: represents the extent to which a method is used in practice.

While the MEM has six constructs, there are instances when some of the MEM constructs may not be relevant or even applicable (Condori-Fernandez and Pastor, 2006; Moody, 2003; Paz et al., 2015; Recker et al., 2005). In this research, we focused on the perception and intention-based constructs - See Fig. 3 below.

The perception and intention-based constructs, known as the MAM, are present in all successful methods (Moody, 2003; Paz et al., 2015). Our objective was to test the SOC-AAM against those constructs. Our strategy is similar to the works of Recker et al. (2005), Paz et al. (2018, 2015), and Díaz et al. (2021). Abrahão et al. (2004) state that one of the major advantages of using the MAM and the associated measurement scales is that it is based on previous studies where similar surveys were used and validated in the context of method adoption. We do not use the 'Actual Usage' and 'Actual Efficacy' constructs from the MEM for the reasons outlined below.

Firstly, Moody (2003), states that it is not possible to assess 'Actual Usage' under experimental conditions. Given that our testing and evaluation was conducted as an experiment, it was not feasible to test the 'Actual Usage' construct. However, an intention to use a particular method can be a predictor of 'Actual Usage' (Paz et al., 2015; Recker et al., 2005). Although we do not include the 'Actual Usage' construct in the evaluation, we argue that an expression of intent by SOC practitioners to use the SOC-AAM in future indicates the likelihood of the SOC-AAM being adopted in practice.

Secondly, Moody (2003) emphasises that the use of the 'Actual Efficacy' constructs are only meaningful when comparing between different methods. Given that the SOC-AAM is a new, and to the best of the researchers' knowledge, the only existing systematic method for capturing the performance of an analyst based on multiple SOC functions, it was not possible to compare it with another systematic method to justify the use of the 'Actual Efficacy' constructs. This study, therefore, does not use these two constructs.

In addition to the perception and intention-based constructs, we also solicited the opinions of the experts on the perceived completeness (PC) of the SOC-AAM (Paz et al., 2015; 2013). We define 'PC' as the extent to which a SOC expert believes that the SOC-AAM covers all aspects of analyst functions (Paz et al., 2015). Also, we solicited the opinions of the SOC managers and analysts to ascertain whether the use of the SOC-AAM as the evaluation tool resulted in improved performance. Lastly, we also asked SOC managers to provide feedback on whether the scores achieved by their analysts during the experiment reflected the manager's perception of the contribution of each analyst within the team.

7.1. Testing of the SOC-AAM

The testing and evaluation of the SOC-AAM took place at two different organisations. The evaluation was guided by the following research questions, which were developed based on the MEM/MAM, as explained earlier:

- (RQ1) Do SOC managers and analysts consider the SOC-AAM as easy-to-use and useful?
- (RQ2) Would SOC managers and analysts use the SOC-AAM in practice in the future?
- (RQ3) According to the SOC managers and analysts, to what extent does the SOC-AAM cover all the main functions of an analyst?
- (RQ4) According to the SOC managers and analysts, did the introduction of the SOC-AAM lead to an improvement of an analyst's performance?
- (RQ5) According to SOC managers, did the final performance score(s) of analysts within their team reflect the manager's perceived performance of each analyst?

To protect the identity of the participants and the organisation where the evaluation took place, we refer to the two organisations as Corp1-SOC and Corp2-SOC. Both organisations were 'purposively' (Ogbeifun et al., 2016) selected through opportunity and agreement with the senior managers. Participants from both SOCs were given a participant information sheet outlining the purpose of the study. The participant information sheet detailed the participants' rights, and they were free to choose whether or not to participate in the study.

Corp1-SOC provides a 24x7 security monitoring and response service for its own organisation and also offers SOC services as a Managed Service Security Provider (MSSP) to a number of other

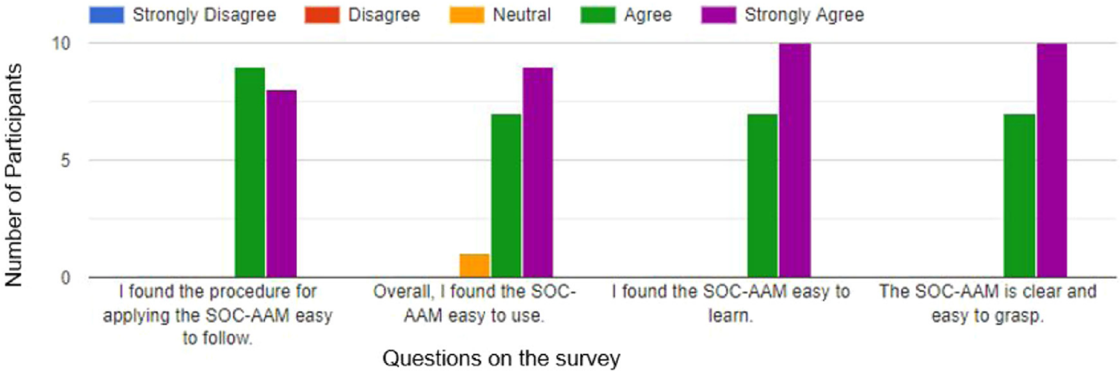

Fig. 4. Response breakdown regarding the PEOU.

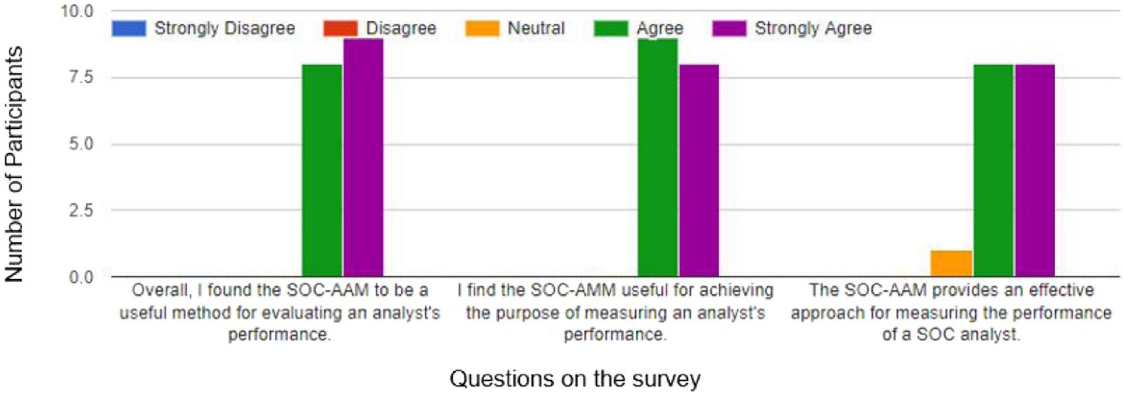

Fig. 5. Response breakdown regarding the PU.

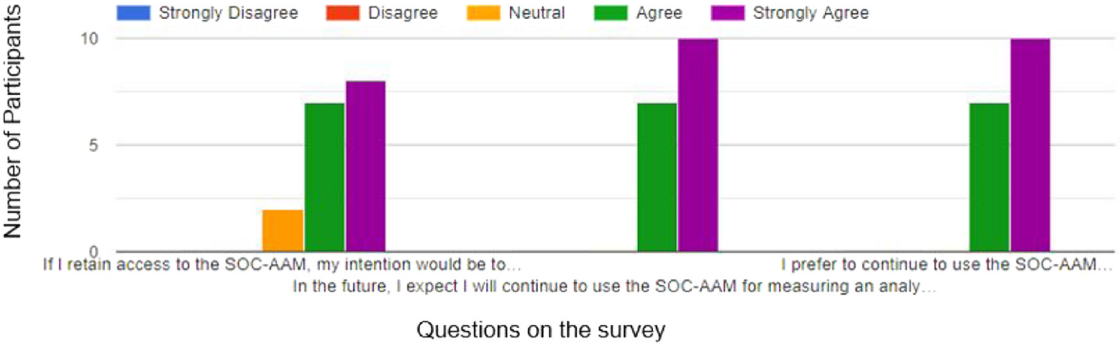

Fig. 6. Response breakdown regarding the ItU.

organisations in the United Kingdom and across Europe. Analysts who work in Corp1-SOC perform the range of SOC functions as detailed in Table 1 above. Thirteen analysts, together with the team manager at Corp1-SOC, agreed to participate in the study without any reward for their participation.

Corp2-SOC, on the other hand, runs an internal SOC for a Norwegian telecommunication company. Analysts who work at Corp2-SOC also undertake a wide range of SOC functions as detailed in Table 1 above. Following a discussion with senior managers at Corp2-SOC, two analysts and their SOC manager agreed participate in the testing and evaluation of the SOC-AAM.

The SOC-AAM tool has an accompanying ‘Read Me’ notes which detail a step by step process regarding how to use it as described above. In addition, the managers from both SOCs were presented with a practical demonstration of the SOC-AAM via Zoom by the first author. During the demonstration, hypothetical KPIs values were used to facilitate the explanation of the evaluation process.

During the evaluation experiment, monthly meetings were held with the SOC managers via Zoom to discuss issues that may have risen while using the SOC-AAM. The meeting provided an additional opportunity to ascertain the ground truth on the weights assigned to different functions. As part of the evaluation process, analysts from both SOCs were given the SOC-AAM template by their respective managers to record their output in the areas of measures, apart from the quality of their analysis and the quality of their report. The SOC managers provided us with anonymised scores of their analysts at the end of each month. Appendix D - Table 17 shows the monthly individual breakdown scores by one of the analyst at Corp2-SOC.

7.2. Post-testing feedback

After four months of testing, the participants were invited to participate in a post-task survey. The purpose of the survey was to

Table 5
Adopted measurement items for the study.

Construct	Adopted construct definition	No	Item	References
Perceived Usefulness (PU)	The extent to which a person believes that the SOC-AAM will be effective for evaluating the performance of an analyst.	PU1	Overall, I found the SOC-AAM to be a useful method for evaluating an analyst's performance.	Adopted from: Moody (2003)(PU4, Q7) Recker (2008) (PU1, Q1) Davis (1989) (PU14)
		PU2	I find the SOC-AMM useful for achieving the purpose of measuring an analyst's performance.	Adopted from: Recker (2008) (PU2, Q2)
		PU3	The SOC-AAM provides an effective approach for measuring the performance of a SOC analyst.	Adopted from: Moody (2003)(PU6, Q12)
Perceived Ease of Use (PEOU)	The extent to which a person believes that using the SOC-AAM would be free of effort.	PEOU1	I found the procedure for applying the SOC-AAM easy to follow.	Adopted from: Moody (2003)(PEOU1, Q1) Davis (1989) (PEOU14)
		PEOU2	Overall, I found the SOC-AAM easy to use.	Adopted from: Moody (2003)(PEOU1, Q4) Recker (2008)(PEOU1, Q1) Davis (1989) (PEOU8)
		PEOU3	I found the SOC-AAM easy to learn.	Adopted from: Moody (2003)(PEOU3, Q6) Recker (2008)(PEOU1, Q2) Cherdantseva (2014) (PEOU1, Q26)
		PEOU4	The SOC-AAM is clear and easy to grasp.	Adopted from: Moody (2003)(PEOU5, Q11) Cherdantseva (2014) (PEOU2, Q33)

ascertain the opinion of the study participants on the PEOU, PU, ItU and PC of the SOC-AAM. The survey also had two questions specifically designed to find out: (1) whether the introduction of the SOC-AAM resulted in an improvement of performance, and (2) whether the SOC managers believed the score achieved by an analyst during the testing period accurately reflected the performance of the analyst.

The perception and intention-based questions for the survey were formulated using a 5-point Likert scale and were based on items synthesised from previous works (Davis, 1989; Davis et al., 1989; Moody, 2003; Paz et al., 2015). The wording of the items were changed to reflect the objectives of the SOC-AAM. For each question, the participants were asked to rate their responses on a scale, ranging from 1 to 5, where 1 denotes an extremely negative perception of the construct, and 5 a very good positive rating. Given that 3 is the midpoint of the 5-point Likert scale, mean scores obtained from the study participants' constructs that are greater than 3 will be considered as positively perceived by the SOC experts. This approach is similar to the work of Paz et al. (2015). The constructs and the original scales adopted for the study Tables 5 and 6.

7.3. Data analysis and results of the post-testing feedback

Seventeen participants in total completed and returned the post-testing survey. The average years of experience for the participants is 4.7 years. The industry breakdown for the participants is: 3 (17.6%) employees from the telecommunication provider, and 14 (82.4%) employees from the Managed Security Service Provider (MSSP). The feedback received from the surveys was analysed and used to answer the research questions defined under Section 7.1.

The Cronbach's alpha was used to assess the reliability and internal consistency of the set of scale items used in the survey. A high level of internal consistency was found with all the constructs, with Cronbach's alpha > 0.7 in all cases (See Table 7). This implies that the items in the questionnaire are highly correlated. Although there is no agreed upon standard for reliability, in the literature, $\alpha \geq 0.7$ are typically considered to be acceptable Moody (2003).

Under the MAM/MEM, a score greater than 3 (the neutral point in a 5-point Likert scale) indicates a positive perception (Gonzalez-Lopez and Bustos, 2019; Paz et al., 2015; Recker et al., 2005). Thus, the aim was to analyse the survey data in order to determine whether the overall perception rating from the participants was greater or less than 3 for the various constructs.

A Shapiro-Wilk normality test revealed that the data from the participants was not normally distributed. Therefore, a non-parametric statistical method was used to test the data. A non-parametric method also fits the data collected because of the small sample size (Gonzalez-Lopez and Bustos, 2019). The Wilcoxon signed-rank test was used to determine whether the median score of the participants was higher than 3 (Gonzalez-Lopez and Bustos, 2019).

A one-sample Wilcoxon signed-rank test revealed that the median of the scores from the participants for both PEOU and PU was significantly greater than 3, a $p < 0.05$, indicating a positive perception of the SOC-AAM from SOC experts. The median scores for the PEOU and PU were 5 and 4 respectively.

An intention to use a particular method is considered as an important factor when evaluating the pragmatic success of a method. The median score from the participants was 5, which is greater than 3 with a $p < 0.05$. Based on the outcome, we conclude that the participants have intentions to use the SOC-AAM in future evaluations.

When asked about how complete they perceived the SOC-AAM as an evaluation tool, the result showed that participants perceived the SOC-AAM as covering the key areas upon which an analyst's performance can be measured. Fig. 7 shows the results of the PC. The median score for the PC is 4, which is greater than 3 with a $p < 0.05$. While the SOC-AAM was initially conceptualised using existing SOC frameworks (Majid and Ariffi, 2019; Onwubiko, 2015; Schinagl et al., 2015) and input from SOC experts obtained through interviews, some of the participants reported in their feedback under research question 4 that analysts could be tasked with work that may take time, but that is not accounted for in the SOC-AAM. All the same, our goal was to propose an approach based on the most common analyst's functions as reported by the SOC experts in our earlier work (Agyepong et al., 2020b) and insight from the existing literature (Onwubiko, 2015; Schinagl et al., 2015). We recognise this as a limitation in our work.

When the participants were asked whether the use of the SOC-AAM resulted in an improvement, the majority of the analysts

Table 6
Adopted measurement items for the study.

Construct	Adopted construct definition	No	Item	References
Intention to Use (ItU)	The extent to which a person intends to continue to use the SOC-AAM for the evaluation of an analyst performance.	ItU1	If I retain access to the SOC-AAM, my intention would be to continue to use it when evaluating analysts' performance.	Adopted from: Recker (2008) (ItU1, Q1)
		ItU2	In the future, I expect I will continue to use the SOC-AAM for measuring an analyst's performance.	Adopted from: Recker (2008) (ItU2)
		ItU3	I prefer to continue to use the SOC-AAM for the measuring of an analyst's performance over other ways of assessing an analyst's performance.	Adopted from: Recker (2008) (ItU3) Moody (2003) (ItU2, Q16)
Perceived Completeness (PCO)	The extent to which a person believes that the SOC-AAM covers all core areas in evaluating the performance of an analyst.	PCO1	I found the SOC-AAM to be complete method for measuring the performance of an analyst based on their task performance.	Adopted from: Paz et al. (2015)
		PCO2	I found the SOC-AAM to be complete method for measuring an analyst's performance in comparison to existing approaches.	

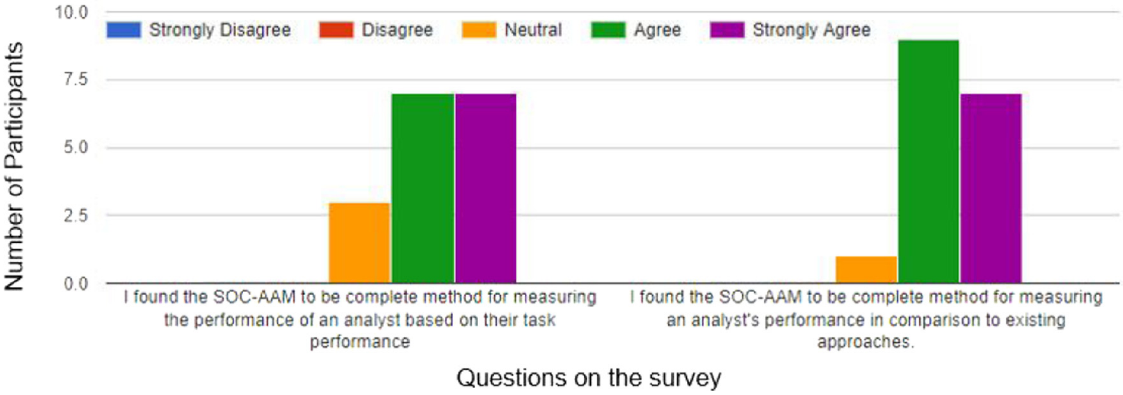

Fig. 7. Response breakdown regarding the PC.

Table 7
Reliability of the scale items.

Construct	**Cronbach's α**
Perceived Ease of Use	0.886
Perceived Usefulness	0.894
Intention to Use	0.899
Perceived Completeness	0.761

(92%) commented that the guidelines have improved their incident reports because it provided relevant cues. The manager at Corp1-SOC commented that:

"The guidelines for assessing the quality of analysts' analysis has been useful to the team. I think it encouraged them to expand their thinking and take a step back to think through what they need to do when writing their incident report. I also believe that the tool made it possible for everyone within the team to understand the basis upon which they are being assessed."

The manager at Corp2-SOC expressed a similar opinion, but suggested that producing a good quality report comes with experience. The manager at Corp2-SOC stated: *"I think the SOC-AAM greatly helped my analysts develop their ability to analyze events. I think the quality of analysis criteria are good but analysis comes with experience, knowledge and also process of the organisation."*

The managers were asked whether the scores achieved by their analysts reflected their perceived view of each individual analyst's contribution within their team. Extracts from the managers' responses are provided below. The manager at the Corp1-SOC stated: *"There are some competitive individuals within the team, so I was expecting those individuals to show that competitiveness. However, looking at the monthly scores, it was great to see that all the analysts did pretty well. I am of the opinion that the scores achieved by each individual analyst reflected in how I perceive their contribution to the team. One area that I saw improvement across the board is report writing."*

The manager at the Corp2-SOC stated that the scores achieved by analysts only reflected about 95% of their performance. According to the Corp2-SOC manager: *"implementation and architect activities are not in the SOC-AAM. Therefore, when the results are collected for each period, there will be times when the outcome will not be linear because the analyst was performing other implementation activities. But overall, when compared to the general SOC, I think the SOC-AAM is satisfactory in measuring analyst performance"*.

The comments indicate that analysts at Corp2-SOC have other tasks that are not measured in the SOC-AAM. However, as stated earlier under Section 3, our intention was to measure analysts' performance on the basis of their most common functions. Besides, there is also no evidence in the literature to suggest that implementation and architectural activities are typical functions expected of analysts (Agyepong et al., 2020b; Onwubiko and Ouazzane, 2019b). So while analysts at Corp2-SOC undertake those activities, this will not be the case in many other SOCs to justify including those activities in our method.

8. Discussion and research implications

The overall objective for this study was to find a systematic approach to evaluating the performance of a SOC analyst. The findings from the experimental case study shows that the SOC-AAM enables SOC managers and stakeholders such as supervisors to aggregate, quantify and evaluate the performance of analysts in a systematic manner.

Our findings and discussions with the SOC practitioners also lead us to believe that the SOC-AAM offers an operational, adaptable and practical method to evaluating analysts' performance. It is operational because it can be applied, as it is, by any SOC offering the functions identified by the SOC-AAM to evaluate the performance of an analyst (Onwubiko, 2020). It is adaptable and practicable because it can be used to suit each SOC's specific situation and as per the functions offered by a SOC. Also, given that the SOC-AAM covers the main functions expected of an analyst (Agyepong et al., 2020b), it provides a comprehensive approach when seeking to evaluate the performance of an analyst. Nevertheless, the number of participants in the study was small, making it difficult generalise outcome of the experimental case study.

While the sample size of the experimental case study makes generalisation of the findings difficult, as stated by (Yin, 2018), the aim of a case study is not to generalise but rather to get deeper understandings of a specific situation. Thus, the objective of the testing was to assess the efficacy of the SOC-AAM from practitioners point of view as a method for evaluating analysts performance.

In comparison to existing performance metrics that are based on KPIs, which generally do not differentiate the efforts of analysts (Onwubiko, 2015; Sundaramurthy et al., 2015; 2014), the weights proposed by this study allow SOC managers to differentiate efforts. We make a distinction between the priority of alerts actioned by analysts and, thereby, contribute to solving the current problem that usually does not consider priority (Kokulu et al., 2019). Also, the SOC-AAM considers several aspects of analysts' tasks and previously unmeasured areas, such as dealing with false positives (Sundaramurthy et al., 2015).

Given that different SOCs provide different functions (Jacobs et al., 2013; Onwubiko, 2015; Schinagl et al., 2015), and analyst responsibilities vary between SOCs (Goodall et al., 2004), this study acknowledges that each analyst performs only a subset of the functions presented in the SOC-AAM. While some SOC researchers have attempted to organise analyst responsibilities based on the tiers in which they operate (1,2,3) (Kokulu et al., 2019; Vielberth et al., 2020), there are often inconsistencies in the responsibilities assigned to the tiers. Onwubiko and Ouazzane (2019a), on the other hand, only describe the roles of analysts without assigning them to a specific tier. These researchers consider all analyst functions to be the generic functions one would anticipate from an analyst. Similarly, Aung et al. (2020) and Li et al. (2016) discuss how analysts apply patches to fix vulnerabilities without assigning them to a particular tier. Also, analysts working for an in-house SOC (a SOC that is owned by the organisation it is protecting) may have different functions in comparison with analysts working for a SOC that offers its services as a Managed Security Service Provider (MSSP). MSSPs are typically third-party organisations that provide SOC services under a specific contract to another organisation. However, as noted in the existing literature (Jacobs et al., 2013; Zimmerman, 2014), both in-house and third-party SOCs offer a wide range of functions as detailed in the SOC-AAM.

The inconsistency and current lack of consensus on the precise expectations of functions of an analyst at each tier influenced our decision not to assign specific tasks to the tiers 1, 2, and 3 in the SOC-AAM, but present a broad range of functions, allowing the performance to be measured based on the specific set of functions offered by a SOC.

The SOC-AAM does not make a distinction between analyst tiers, and hence is more applicable in the context of a SOC with a non-hierarchical structure, where all analysts are expected to have the same level of skills, perform the same functions and work independently (Alharbi, 2020; Kokulu et al., 2019). When using the SOC-AAM, SOC managers may customise the framework and choose to evaluate analysts only in relation to specific relevant functions. SOC managers and analysts should agree on assessment areas in both hierarchical and non-hierarchical contexts. Also, SOC managers could choose to compare the scores of analysts operating at the same tier as a part of each assessment.

Another benefit to the proposed approach is the provision of novel guidelines for assessing the quality of an analyst's analysis and their incident report as a part of an analyst's performance evaluation process. To the best of our knowledge, this is the first research to work collaboratively with industry experts to propose formal guidelines for assessing the quality of an incident analysis/report. Using the proposed guidelines, it is anticipated that novice or junior analysts can improve their performance when it comes to the analysis function. In addition, SOC managers can use these guidelines to assess the performance of analysts in this qualitative based area which traditional is difficult to evaluate (Achraf Chamkar et al., 2021).

Even though this study demonstrates that it is feasible to measure an analyst's performance using a systematic approach, the pairwise comparison conducted as part of the AHP is a time-consuming activity. Thus, a contribution of this work is to simplify this process by proposing the weights that SOC managers and stakeholders can use to evaluate the performance of an analyst. SOC managers and stakeholders do not have to go through the intense AHP process. The proposed weights can be used, as there is a consensus from the experts. One area of concern is whether the opinions and weights deduced by a small group of experts can be unconditionally generalised to all contexts and organisations. We recognise this as a potential issue and therefore attempted to lessen this concern by engaging with experts from five different industries. Moreover, to avoid bias in the pairwise judgement, the Delphi method was used over other group data collection method such as a focus group to ensure that a dominant participant do not hijack the session (Brown, 2018).

From a research perspective, this study offers a detailed insight into the work of analysts, and as such, cyber security researchers who may not have access to SOCs can draw on this study to understand the operations of cyber analysts. The areas of measures presented in this work would be valuable to SOC system designers who can draw on the suggested areas of measures when designing systems for SOCs to facilitate the evaluation of an analyst performance. For example, analysts' monitoring dashboards for tools such as Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDSs) can be designed to incorporate some of the performance metrics proposed in this study to capture analysts' performance. Dashboards are interfaces that bring together several security tools on one screen for an analyst.

9. Conclusion and future work

Evaluating the performance of a SOC analyst is a subject of interest for both cyber security researchers and practitioners, as a poor performance from analysts will negatively impact on the overall effectiveness and efficiency of a SOC. However, existing literature highlights the lack of a systematic approach for evaluating the performance of an analyst, causing frustration for both SOC managers and analysts.

In this paper, we proposed a systematic method for evaluating the performance of analysts consistently and systematically by drawing on a Delphi panel and the principles of the AHP. Our work represents a potential change in direction in how analysts' performance is evaluated. We have demonstrated that it is possible to evaluate the performance of an analyst in a systematic manner based on their task performance by proposing a weighted approach. To the best of our knowledge, this is the first empirical study to propose a systematic approach for evaluating the performance of an analyst.

This study has some limitations in that we focus on analysts' task performance. We recognise that individual work performance can be evaluated from other dimensions such as adaptive performance and contextual performance (Koopmans, 2014). Future work may be to investigate how to capture the performance of an analyst based on other dimensions. Also, some participants described the SOC-AAM as time-consuming and advised combining it with their ticketing systems, such as Jira, to streamline the evaluation process. Working with SOC system designers to integrate the proposed technique into SOC tooling to assist the evaluation could be a potential solution to this constraint. Another limitation of this study is the manager's random selection of a written report as part of the evaluation process. An incident report that is inadequately or poorly written may be missed by the manager. Furthermore, the functions and roles of analysts used in this work are based on a case study conducted with a small number of participants (SOC experts) who selected and validated the functions in a prior work and insights from existing literature that describes the primary function of a SOC (Majid and Ariffi, 2019; Onwubiko, 2015; Schinagl et al., 2015). Therefore, we recognise that the small sample size may have led to the omission of certain functions. Additionally, a different group of participants may have chosen or included additional analyst functions.

Ethical Approval

This research was approved by Cardiff University's Research Ethics Committee (Approval ID: COMSC/Ethics/2019/063).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Enoch Agyepong: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Yulia Cherdantseva:** Conceptualization, Methodology, Resources, Supervision, Validation, Writing – review & editing. **Philipp Reinecke:** Resources, Supervision, Validation, Writing – review & editing. **Pete Burnap:** Resources, Supervision, Validation, Writing – review & editing.

Acknowledgement

We express our gratitude to all the participants who took part in this study. Without their insight, this work would not have been possible. We will also like to thank the anonymous reviewers for their valuable feedback.

Appendix A. Decision Matrices for the Criteria and Subcriteria

Table 8
Weights and Consistency Ratio (CR) for the Main Evaluation Criteria.

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

Table 9
Weights and Consistency Ratio (CR) for the Monitoring and Detection Function Subcriteria.

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

Table 10
Weights and Consistency Ratio (CR) for the Analysis Function Subcriteria.

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

Table 11
Weights and Consistency Ratio (CR) for the Baseline and Vulnerability Function Subcriteria.

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

Table 12
Weights and Consistency Ratio (CR) for the Intelligence Function Subcriteria.

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

Table 13
Weights and Consistency Ratio (CR) for the Response and Reporting Function Subcriteria.

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

Table 14
Weights and Consistency Ratio (CR) for the Policies and Signature Management Subcriteria.

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

Appendix B. Final Weights

Table 15
Global Priority: Final Weight for Each Task.

Criteria and Subcriteria	Criteria Weights	Subcriteria Weights	**Global weight = the weight of each criterion(×)their respective subcriterion weight**	**Global Weights(×)100**
Monitoring and Detection Function	0.2494			
Number of Misconfiguration Detected over a rolling period		0.0507	0.0126	1.2640
Number of Critical Incidents Detected over a rolling period		0.2001	0.0499	4.9901
Number of High Incidents Detected over a rolling period		0.1390	0.0347	3.4677
Number of Medium Incidents Detected over a rolling period		0.0972	0.0242	2.4249
Number of Low Incidents Detected over a rolling period		0.0442	0.0110	1.1013
Number of Use Case Incidents Detected over a rolling period		0.1262	0.0315	3.1470
Number of Zero Day Incidents Detected over a rolling period		0.3427	0.0855	8.5479
Analysis Function	0.2450			
Quality of Analysis		0.4427	0.1084	10.8440
Number of Critical Priority Alert Analysed over a rolling period		0.1091	0.0267	2.6716
Number of High Priority Alert Analysed over a rolling period		0.0974	0.0239	2.3866
Number of Medium Priority Alert Analysed over a rolling period		0.0640	0.0157	1.5667
Number of Low Priority Alert Analysed over a rolling period		0.0416	0.0102	1.0180
Number of In-house Use case Analysed over a rolling period		0.0910	0.0223	2.2288
Number of Zero Day Incidents Analysed over a day rolling period		0.1544	0.0378	3.7817
Baseline and Vulnerability Function	0.1084			
Number of Patches Applied over a rolling period		0.3873	0.0420	4.1982
Number of Patches Rolled back over a rolling period		0.1698	0.0184	1.8410
Number of Vulnerabilities Discovered over a rolling period		0.4429	0.0480	4.8004
Intelligence Function	0.1302			
Number of Use Cases Created over a rolling period		0.3873	0.0504	5.0432
Number of Indicators of Compromised (IOCs) Implemented over a rolling period		0.4429	0.0577	5.7666
Number of Indicators of Compromised (IOCs) Shared over a rolling period		0.1698	0.0221	2.2116
Response and Reporting Function	0.1769			
Quality of Incident Report		0.3641	0.0644	6.4403
Number of False Positives Reported over a rolling period		0.0468	0.0083	0.8276
Number of True Critical Incident Closed over a rolling period		0.1090	0.0193	1.9277
Number of True High Incident Closed over a rolling period		0.0995	0.0176	1.7594
Number of True Medium Incident Closed over a rolling period		0.0648	0.0115	1.1455
Number of True Low Incident Closed over a rolling period		0.0516	0.0091	0.9129
Number of In-house Use Case Incidents Closed over a rolling period		0.0781	0.0138	1.3817
Number of Zero Day Closed over a rolling period		0.1862	0.0329	3.2930
Policies and Signature Function	0.0901			
Number of Use Cases Created over a rolling period		0.2500	0.0225	2.2527
Number of Indicators of Compromised (IOCs) Implemented over a rolling period		0.5000	0.0451	4.5053
Number of Indicators of Compromised (IOCs) Shared over a rolling period		0.2500	0.0225	2.2527
Total Weight			1	100

Appendix C. A Security Operations Centre Analyst Assessment Method

Table 16
An Analyst Assessment Template.

ANALYSTS FUNCTIONS AND KPI(s)	WEIGHTS	ANALYST'S KPI SCORE	ANALYST'S SCORE PER ACTIVITY	TEAM'S TOTAL KPI	TEAM'S OVERALL SCORE
Monitoring and Detection Function					
Number of Misconfiguration Detected over a rolling period	1.2640				
Number of Critical Incidents Detected over a rolling period	4.9901				
Number of High Incidents Detected over a rolling period	3.4677				
Number of Medium Incidents Detected over a rolling period	2.4249				
Number of Low Incidents Detected over a rolling period	1.1013				
Number of Use Case Incidents Detected over a rolling period	3.1470				
Number of Zero Day Incidents Detected over a rolling period	8.5479				
Analysis Function					
Quality of Analysis	10.8440				
Number of Critical Priority Alert Analysed over a rolling period	2.6716				
Number of High Priority Alert Analysed over a rolling period	2.3866				
Number of Medium Priority Alert Analysed over a rolling period	1.5667				
Number of Low Priority Alert Analysed over a rolling period	1.0180				
Number of In-house Use case Analysed over a rolling period	2.2288				
Number of Zero Day Incidents Analysed over a day rolling period	3.7817				
Baseline and Vulnerability Function					
Number of Patches Applied over a rolling period	4.1982				
Number of Patches Rolled back over a rolling period	1.8410				
Number of Vulnerabilities Discovered over a rolling period	4.8004				
Intelligence Function					
Number of Use Cases Created over a rolling period	5.0432				
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	5.7666				
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2116				
Response and Reporting Function					
Quality of Incident Report	6.4403				
Number of False Positives Reported over a rolling period	0.8276				
Number of True Critical Incident Closed over a rolling period	1.9277				
Number of True High Incident Closed over a rolling period	1.7594				
Number of True Medium Incident Closed over a rolling period	1.1455				
Number of True Low Incident Closed over a rolling period	0.9129				
Number of In-house Use Case Incidents Closed over a rolling period	1.3817				
Number of Zero Day Closed over a rolling period	3.2930				
Policies and Signature Function					
Number of Use Cases Created over a rolling period	2.2527				
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	4.5053				
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2527				
Total Weight	100				
Analyst's Overall Score					
Team's Overall Score					
Individual Analyst Percentage Contribution (%)					
Team's Percentage Contribution (%)					

Appendix D. Performance Evaluation Score: Corp2 - Analyst 1

Table 17
Corp2 - Analyst 1.

ANALYSTS FUNCTIONS AND KPI(s)	WEIGHTS	ANALYST'S KPI SCORE	ANALYST'S SCORE PER ACTIVITY	TEAM'S TOTAL KPI	TEAM'S OVERALL SCORE
Monitoring and Detection Function					
Number of Misconfiguration Detected over a rolling period	1.2640	2	2.5280	4	5.0560
Number of Critical Incidents Detected over a rolling period	4.9901	0	0.0000	0	0.0000
Number of High Incidents Detected over a rolling period	3.4677	3	10.4031	5	17.3384
Number of Medium Incidents Detected over a rolling period	2.4249	11	26.6741	21	50.9234
Number of Low Incidents Detected over a rolling period	1.1013	20	22.0255	48	52.8612
Number of Use Case Incidents Detected over a rolling period	3.1470	2	6.2940	2	6.2940
Number of Zero Day Incidents Detected over a rolling period	8.5479	1	8.5479	2	17.0959
Analysis Function					
Quality of Analysis	10.8440	7	75.9082	14	151.8164
Number of Critical Priority Alert Analysed over a rolling period	2.6716	0	0.0000	0	0.0000
Number of High Priority Alert Analysed over a rolling period	2.3866	3	7.1598	5	11.9330
Number of Medium Priority Alert Analysed over a rolling period	1.5667	11	17.2333	21	32.8999
Number of Low Priority Alert Analysed over a rolling period	1.0180	20	20.3591	48	48.8619
Number of In-house Use case Analysed over a rolling period	2.2288	2	4.4575	2	4.4575
Number of Zero Day Incidents Analysed over a day rolling period	3.7817	1	3.7817	2	7.5634
Baseline and Vulnerability Function					
Number of Patches Applied over a rolling period	4.1982	28	117.5491	40	167.9273
Number of Patches Rolled back over a rolling period	1.8410	3	5.5230	5	9.2050
Number of Vulnerabilities Discovered over a rolling period	4.8004	29	139.2111	38	182.4145
Intelligence Function					
Number of Use Cases Created over a rolling period	5.0432	2	10.0864	3	15.1296
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	5.7666	6	34.5997	8	46.1329
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2116	6	13.2694	8	17.6926
Response and Reporting Function					
Quality of Incident Report	6.4403	7	45.0820	14	90.1641
Number of False Positives Reported over a rolling period	0.8276	0	0.0000	10	8.2761
Number of True Critical Incident Closed over a rolling period	1.9277	0	0.0000	0	0.0000
Number of True High Incident Closed over a rolling period	1.7594	3	5.2781	5	8.7968
Number of True Medium Incident Closed over a rolling period	1.1455	11	12.6004	21	24.0552
Number of True Low Incident Closed over a rolling period	0.9129	20	18.2580	38	34.6903
Number of In-house Use Case Incidents Closed over a rolling period	1.3817	2	2.7635	2	2.7635
Number of Zero Day Closed over a rolling period	3.2930	1	3.2930	2	6.5860
Policies and Signature Function					
Number of Use Cases Created over a rolling period	2.2527	0	0.0000	0	0.0000
Number of Indicators of Compromised (IOCs) Implemented over a rolling period	4.5053	0	0.0000	2	9.0107
Number of Indicators of Compromised (IOCs) Shared over a rolling period	2.2527	0	0.0000	1	2.2527
Total	100				
Analyst's Overall Score					612.8860
Team's Overall Score					1032.1983
Individual Analyst Percentage Contribution (%)					59.3768
Team's Percentage Contribution (%)					100

References

Abrahão, S., Pastor, O., Poels, G., 2004. Comparative Evaluation of Functional Size Measurement Methods: An Experimental Analysis.

Achraf Chamkar, S., Maleh, Y., Gherabi, N., 2021. The human factor capabilities in Security Operation Centre (SOC). The EDP Audit, Control, and Security Newsletter doi:10.1080/07366981.2021.1977026.

Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P., 2019. 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.

Agyepong, E., Cherdantseva, Y., Reinecke, P., Burnap, P., 2020. Cyber Security Operations Centre Concepts and Implementation. In: Yaokumah, W., Rajarajan, M., Abdulai, J.-D., Wiafe, I., Katsriku, F.A. (Eds.), Modern Theories and Practices for Cyber Ethics and Security Compliance. IGI Global, Hershey, PA doi:10.4018/978-1-7998-3149-5.

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

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L., 2021. Cybersecurity incident response in organizations: an exploratory case study and process model of situation awareness. Computers & Security 101, 102–122. https://doi.org/10.1016/j.cose.2020.102122

Ahmed, R.K.A., 2016. Overview of security metrics. Software Engineering 4 (4), 59–64. doi:10.11648/j.se.20160404.11.

Akins, R.B., Tolson, H., Cole, B.R., 2005. Stability of response characteristics of a Delphi panel: application of bootstrap data expansion. BMC Med Res Methodol 5 (1), 37. doi:10.1186/1471-2288-5-37.

Alharbi, S.A., 2020. A qualitative study on security operations centers in saudi arabia: challenges and research directions. J Theor Appl Inf Technol 98 (24), 3972–3982.

Andrade, R.O., Yoo, S.G., 2019. Cognitive security: a comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications 48, 102352. doi:10.1016/j.jisa.2019.06.008.

Arof, A.M., 2015. The application of a combined delphi-AHP method in maritime transport research-A review. Asian Soc Sci 11 (23), 73–82. doi:10.5539/ass.v11n23p73.

Aung, W.P., Lwin, H.H., Lin, K.K., 2020. Developing and analysis of cyber security models for security operation center in Myanmar. In: 2020 IEEE Conference on Computer Applications(ICCA). IEEE, Yangon, Myanmar, pp. 1–6. doi:10.1109/ICCA49400.2020.9022821.

Axon, L., Nurse, J.R.C., Goldsmith, M., Creese, S., 2017. A formalised approach to designing sonification systems for network-security monitoring. International Journal on Advances in Security 10. www.iaria.org

Badie, N., Lashkari, A.H., 2012. A new evaluation criteria for effective security awareness in computer risk management based on AHP. Journal of Basic and Applied Scientific Research 2 (9), 9331–9347.

Benítez, J., Delgado-Galván, X., Gutiérrez, J.A., Izquierdo, J., 2011. Balancing consistency and expert judgment in AHP. Math Comput Model 54 (7–8), 1785–1790. doi:10.1016/j.mcm.2010.12.023.

Brown, J., 2018. Interviews, Focus Groups and Delphi Techniques. In: Brough, P. (Ed.), Advanced Research Methods for Applied Psychology: Design, Analysis and Reporting. Routledge, London, pp. 95–106. https://eprints.lse.ac.uk/

Cherdantseva, Y., 2014. Secure * BPMN - a graphical extension for BPMN 2. 0 based on a Reference Model of Information Assurance & Security. Cardiff University.

Cho, S.Y., Happa, J., Creese, S., 2020. Capturing tacit knowledge in security operation centers. IEEE Access 8. 42021–42041

Condori-Fernandez, N., Pastor, O., 2006. Re-assessing the intention to use a measurement procedure based on COSMIC-FFP. In: International Conference on Software Process and Product Measurement, Valencia, p. 63.

Costa, C., Santos, M.Y., 2017. A conceptual model for the professional profile of a data scientist. In: World Conference on Information Systems and Technologies. Springer, Cham, pp. 453–463. doi:10.1007/978-3-319-56538-5_46.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., Roth, E., 2005. Achieving cyber defense situational awareness: acognitive task analysis of information assurance analysts. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 49 (3), 229–233. doi:10.1177/154193120504900304.

Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly: Management Information Systems 13 (3), 319–339. doi:10.2307/249008.

Davis, F.D., Bagozzi, R.P., Warshaw, P.R., 1989. User acceptance of computer technology: a comparison of two theoretical models. Manage Sci 35 (8), 982–1003.

De Felice, F., Petrillo, A., 2013. Absolute measurement with analytic hierarchy process: a case study for italian racecourse. International Journal of Applied Decision Sciences 6 (3), 209–227. doi:10.1504/IJADS.2013.054931.

Díaz, J., López, J.A., Sepúlveda, S., Villegas, G.M.R., Ahumada, D., Moreira, F., 2021. Evaluating aspects of usability in video game-based programming learning platforms. Procedia Comput Sci 181, 247–254. doi:10.1016/J.PROCS.2021.01.141.

Engeström, Y., 2015. Learning by expanding: an activity-theoretical approach to developmental research, 2nd ed Cambridge University Press doi:10.1017/CBO9781139814744.

, 1999. In: Engeström, Y., Miettinen, R., Punamäki, R.-L. (Eds.), Perspectives on Activity Theory. Cambridge University Press.

Fahmy, H.M., 2001. Reliability evaluation in distributed computing environments using the AHP. Comput. Networks 36 (5–6), 597–615. doi:10.1016/S1389-1286(01)00175-X.

Gan, X., Duanmu, J., Wang, H., 2015. Delphi analysis method and its application in qualitative prediction of aircraft collision unsafe event for air traffic control. In: International Conference on Intelligent Systems Research and Mechatronics Engineering. Atlantis Press, pp. 1472–1475. doi:10.2991/isrme-15.2015.296.

Gonzalez-Lopez, F., Bustos, G., 2019. Evaluating methodologies for business process architecture design-A pilot study. In: ZEUS, pp. 1–8. http://ceur-ws.org/Vol-2339

Goodall, J., Lutters, W., Komlodi, A., 2004. The work of intrusion detection: rethinking the role of security analysts. AMCIS 2004 Proceedings (August) 1421–1427.

Gordon, T.J., 2011. The Delphi Method in futures research methodology-V3.0. The Millenium Project.

Ishizaka, A., Labib, A., 2011. Review of the main developments in the analytic hierarchy process. Expert Syst Appl 38 (11), 14336–14345.

Islam, R., bin Mohd Rasad, S., 2006. Employee performance evaluation by AHP: a case study. Asia Pacific Management Review 11 (3), 16.

Jacobs, P., Arnab, A., Irwin, B., 2013. Classification of Security Operation Centers. In: 2013 Information Security for South Africa. IEEE, pp. 1–7. doi:10.1109/ISSA.2013.6641054.

Jacques Houngbo, P., Toyigbé Hounsou, J., 2015. Measuring information security: understanding and selecting appropriate metrics. International Journal of Computer Science and Security (IJCSS) (9) 108.

Kaplan, R.S., 2009. Measuring Performance: Expert Solutions to Everyday Challenges. Harvard Business Press.

Kokulu, F.B., Bao, T., Doupé, A., Shoshitaishvili, Y., Ahn, G.-J., Zhao, Z., 2019. Matched and mismatched SOCs : a qualitative Study on security operations center issues. Association of Computing Machinery (ACM).

Koopmans, L., 2014. Measuring Individual Performance. Technical Report doi:10.4135/9781483398006.n10.

Li, X., Avellino, P., Janies, J., Collins, M.P., 2016. Software asset analyzer: a system for detecting configuration anomalies. Proceedings - IEEE Military Communications Conference MILCOM 998–1003. doi:10.1109/MILCOM.2016.7795460.

Majid, M.A., Ariffi, K.A.Z., 2019. Success factors for cyber security operation center (SOC) establishment. In: International Conference on Informatics, Engineering, Science and Technology. European Alliance for Innovation (EAI), Bandung doi:10.4108/eai.18-7-2019.2287841.

Miloslavskaya, N., 2018. Information security management in SOCs and SICs. Journal of Intelligent & Fuzzy Systems 35 (3), 2637–2647. doi:10.3233/JIFS-169615.

Moody, D.L., 2003. The method evaluation model: A theoretical model for validating information systems design methods. In: European Conference on Information Systems (ECIS). http://aisel.aisnet.org/ecis2003/79

Mutemwa, M., Mtsweni, J., Zimba, L., 2018. Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. In: 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018. IEEE, Mauritius, pp. 1–6. doi:10.1109/ICONIC.2018.8601251.

O'Connell, T.A., Choong, Y.Y., 2008. Metrics for measuring human interaction with interactive visualizations for information analysis. In: Conference on Human Factors in Computing Systems - Proceedings. ACM, pp. 1493–1496. doi:10.1145/1357054.1357287.

Odu, G., 2019. Weighting methods for multi-criteria decision making technique. Journal of Applied Sciences and Environmental Management 23 (8), 1449. doi:10.4314/jasem.v23i8.7.

Ogbeifun, E., Agwa-Ejon, J., Mbohwa, C., Pretorius, J.H., 2016. The Delphi technique: a credible research methodology. Proceedings of the International Conference on Industrial Engineering and Operations Management 8-10 March, 2004–2009.

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

Onwubiko, C., 2020. Focusing on the recovery aspects of cyber resilience. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020 doi:10.1109/CyberSA49311.2020.9139685.

Onwubiko, C., Onwubiko, A., 2019. Cyber KPI for Return on Security Investment. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, Oxford, UK, pp. 1–8.

Onwubiko, C., Ouazzane, K., 2019. Challenges towards building an effective cyber security operations centre. IJCSA 4 (1), 11–39.

Onwubiko, C., Ouazzane, K., 2019. Cyber onboarding is 'broken'. In: 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019). Institute of Electrical and Electronics Engineers Inc., Oxford, UK, pp. 1–13. doi:10.1109/CyberSecPODS.2019.8885237.

Onwubiko, C., Ouazzane, K., 2019. SOTER: a playbook for cyber security incident management. IEEE Transaction of Engineering and Management 1–22.

Paintsil, E., 2012. Evaluation of privacy and security risks analysis construct for identity management systems. IEEE Syst. J. 7 (2), 189–198. doi:10.1109/JSYST.2012.2221852.

Paz, F., Paz, F.A., Arenas, J.J., Rosas, C., 2018. A perception study of a new set of usability heuristics for transactional web sites. Advances in Intelligent Systems and Computing 722, 620–625. doi:10.1007/978-3-319-73888-8_96.

Paz, F., Paz, F.A., Pow-Sang, J.A., 2015. Experimental case study of new usability heuristics. In: International Conference of Design, User Experience, and Usability. Springer Verlag, pp. 212–223. doi:10.1007/978-3-319-20886-2_21.

Paz, F., Villanueva, D., Rusu, C., Roncagliolo, S., Pow-Sang, J.A., 2013. Experimental evaluation of usability heuristics. Proceedings of the 2013 10th International

Conference on Information Technology: New Generations, ITNG 2013 119–126. doi:10.1109/ITNG.2013.23.

Recker, J., 2008. Understanding Process Modeling Grammer Continuance: A study of the consequences of representational capabilities. Queensland University of Technology.

Recker, J., Rosemann, M., Van der Aalst, W., 2005. On the user perception of configurable reference process models - initial insights. ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems (January) 66.

Saaty, T., 1990. How to make a decision: the analytic hierachy process. Eur J Oper Res 48 (1), 9–26. doi:10.1007/978-1-4419-6281-2_31.

Saaty, T., 2008. Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh, PA.

Saaty, T.L., 1980. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. McGraw-Hill International Book Co.

Saaty, T.L., 2003. Decision-making with the AHP: why is the principal eigenvector necessary. Eur J Oper Res 145 (1), 85–91. doi:10.1016/S0377-2217(02)00227-8.

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

Schlette, D., Vielberth, M., Pernul, G., 2021. CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities. Computers & Security 111, 102482. doi:10.1016/j.cose.2021.102482.

Shah, A., Ganesan, R., Jajodia, S., 2018. A methodology for ensuring fair allocation of CSOC effort for alert investigation. Int. J. Inf. Secur. 18, 1–20. doi:10.1007/s10207-018-0407-3.

Singh Sidhu, S., Singh, K., Singh Ahuja, I., 2020. Ranking of implementation dimensions for maintenance practices in Northern Indian SMEs using integrated AHP-TOPSIS approach. Journal of Small Business And Entrepreneurship 1–20. doi:10.1080/08276331.2020.1809220.

Siregar, K., Siregar, S.F., 2018. Design of mathematical models assessment of working achievements based on spencer competency in PT. Z. IOP Conference Series: Materials Science and Engineering 309 (1). doi:10.1088/1757-899X/309/1/012030.

Smith, M., 2020. The SOC is dead, long live the SOC!. ITNOW 62 (1), 34–35. doi:10.1093/itnow/bwaa015.

Sundaramurthy, S., Ou, X., Bardas, A.G., Case, J., Wesch, M., Mchugh, J., Rajagopalan, S.R., 2015. A human capital model for mitigating security analyst burnout. In: Symposium on Usable Privacy and Security, pp. 347–359.

Sundaramurthy, S.C., Case, J., Truong, T., Zomlot, L., Hoffmann, M., 2014. A tale of three security operation centers. In: Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW '14. ACM, Scottdale, Arizona, pp. 43–50. doi:10.1145/2663887.2663904.

Sundaramurthy, S.C., Mchugh, J., Ou, X., Wesch, M., Bardas, A.G., Mchugh, J., Rajagopalan, S.R., 2016. Turning contradictions into innovations or : how We learned to stop whining and improve security operations. In: the Symposium On Usable Privacy and Security (SOUPS). USENIX, USA, pp. 237–251.

Sundaramurthy, S.C., Wesch, M., Ou, X., McHugh, J., Rajagopalan, S.R., Bardas, A.G., 2017. Humans are dynamic-our tools should be too. IEEE Internet Comput 21 (3), 40–46. doi:10.1109/MIC.2017.52.

Taleai, M., Mansourian, A., 2008. Using delphi-AHP method to survey major factors causing urban plan implementation failure. Journal of Applied Sciences 8 (15), 2746–2751. doi:10.3923/jas.2008.2746.2751.

Turoff, M., Linstone, H.A., 2018. The delphi method: techniques and applications, 2002. Version num{\'e}rique en acc{\'e}s libre: http://is. njit.edu/pubs/delphibook doi:10.2307/3150755.

Vargas, R.V., 2010. Using the analytic hierarchy process (AHP) to select and prioritize projects in a portfolio. In: PMI Global Congress. PA:Project Management Institute, Washington, DC, pp. 1–22.

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security operations center: a systematic survey and open challenges. IEEE Access 8. doi:10.1109/ACCESS.2020.3045514.

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

Zhong, C., Lin, T., Liu, P., Yen, J., Chen, K., 2018. A cyber security data triage operation retrieval system. Computers and Security 76, 12–31. doi:10.1016/j.cose.2018.02.011.

Zhong, C., Yen, J., Liu, P., Erbacher, R.F., 2016. Automate cybersecurity data triage by leveraging human analysts' cognitive process. In: Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S. IEEE, New York, USA, pp. 357–363. doi:10.1109/BigDataSecurity-HPSC-IDS.2016.41.

Zimmerman, C., 2014. Ten strategies of a World-class Cybersecurity Operations Center. The MITRE Corporation. www.mitre.org

Enoch Agyepong is a Cyber Security Architect at Airbus. He is currently a Researcher at the School of Computer Science and Informatics, Cardiff University. His research interest is in Cyber Security and security metrics. He holds a Master's Degree in Advanced Security And Digital Forensics from Edinburgh Napier University, UK and a Bachelors Degree from Greenwich University, London.

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 Ph.D. in Computer Science and an MSc (Hons) in Business Information Systems Design, Russia. Yulia is a cyber skills lead at the School and is interested in cybersecurity education from the primary school up to professional development level. Yulia is passionate about equality and diversity in cybersecurity.

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 Ph.D. in Computer Science from Freie Universität Berlin and an M.Sc. in Computer Science from Humboldt University of Berlin.

Professor 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 Ph.D. in Computer Science from Cardiff University.