UNIVERSITY OF
GLOUCESTERSHIRE

This is a peer-reviewed, post-print (final draft post-refereeing) version of the following published document, © 2024 The Author(s), under exclusive license to Springer Nature Switzerland AG. All Rights Reserved and is licensed under All Rights Reserved license:

Zidan, Kamal ORCID logoORCID: https://orcid.org/0000-0002-6523-2924, Alam, Abu ORCID logoORCID: https://orcid.org/0000-0002-5958-7905, Allison, Jordan ORCID logoORCID: https://orcid.org/0000-0001-8513-4646 and Al-Sherbaz, Ali ORCID logoORCID: https://orcid.org/0000-0002-0995-1262 (2024) Assessing the Challenges Faced by Security Operations Centres (SOC). In: Future of Information and Communication Conference (FICC), 4-5th April 2024, Berlin, Germany. ISSN 2367-3370 ISBN 9783031539633

Official URL: http://dx.doi.org/10.1007/978-3-031-53963-3_18
DOI: http://dx.doi.org/10.1007/978-3-031-53963-3_18
EPrint URI: https://eprints.glos.ac.uk/id/eprint/13843

Disclaimer

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

Assessing the Challenges faced by Security Operations Centres (SOC)

Kamal Zidan[1], Abu Alam[2] Jordan Allison, and Ali Al-sherbaz

University of Gloucestershire, Cheltenham, United Kingdom,
kzidan1@glos.ac.uk

Abstract. *Cyber security threats are increasing rapidly, and due to this organisations are utilising Security Operations Centres(SOC) to monitor their network and to observe activities by collecting data about malicious events and behaviours. The main purpose of SOC is to defend organisations assets by spotting potential malicious activities. There are number of challenges that SOC team face on daily based. Hence, the question of this study is* ***'What are the main challenges faced by SOC analysts and how their impact on organisations?'****. This paper presents the outcome of interviews that have been carried out with SOC specialists in UK to understand the main challenges they face. The interviewed individuals are from different types and sizes of organisations. Hence, they have indicated various challenges when working with SOC. Skills shortages, False positives, Lack of automation, poor communication between SOC analysts and board level implications are the most highlighted difficulties amongst participants whilst working with SOC.*

Keywords: Cyber Security, Security Operations Centre, Analysts

1 Introduction

The changing current environment of technology requires security measures to be in place for IT assets including software, machines and networks that can work collectively and collaboratively to provide systems for businesses and organisations to serve their clients and customers. Cyber Security measures are required more than ever to increase the security posture [1].

Organisations are moving towards the reliance on technology to improve their operations and activities. Since the revolution of the internet, cyber security has always been an essential matter to be highlighted specially with Covid19 outbreak where cyber threats have resulted of unwanted consequences as almost everyone has moved to work remotely. One of the problems is that threats actors can always take advantage of any gaps or vulnerabilities to achieve their malicious aims and goals. Specially for organisations users working remotely, issues such as using public network and less secure services can expose them to cyber-attacks.Hence, security threats have occurred and will always arise in the future [2].

According to Deliotte 2022 trends report [2], added that the emerging types of technologies will lead organisations to think about enhancing their infrastructure and upskilling their employees. The emerging technologies includes the share of data and cyber security. The share of data has become a process that provides knowledge for organisations. The exponential growth of data sharing exposes cyber-attacks which in turn lead security teams that are responsible of defending systems to be swamped and overwhelmed with number and sophistication of cyber security threats. Thus, cyber security teams are consuming a lot of time and resources in order to monitor and identify security events.

Due to the widespread of threats [1] organisations need to implement defence approaches. Majid and Ariffi [1] added that SOC can be a significant mechanism to monitor and defend against cyber threats that can damage a firm.

SOC is a unit that is used for events detection and responding to incidents that are associated with cyber security threats via monitoring, detecting, examining and reporting on anomalies [3]. Well-known, unknown and new activities are part of SOC tasks that organisations looking to have in their security environment. There are variety of reasons that firms and organisations must utilise SOC such as situations awareness including hardware and software assets. Also, controlling vulnerabilities, threat detection and prevention where SOC provide the ability to detect when an unauthorised individual has breached a specific asset plus its capabilities of identifying vulnerabilities on the monitored estates [4].

The primary research question of this study ***'What are the main challenges faced by SOC analysts and how they impact on organisations?'*** was answered by conducting interviews with SOC specialists in the UK and analysing qualitative and quantitative data collected from interviews. This paper focuses on understanding and assessing SOC challenges that are faced by organisations. It also links challenges between previous academic literature and industrial point of view.

2 Related Works

The categories of SOC include analysts, processes and technology. SOC analysts and specialists require to have skills in regards to understanding the organisations polices and how network devices operate. They are also responsible of making decision on whether an attack is real or fake in order to implement an effective responding plan [5]. Therefore, processes include an organisation policies, standards and methods that need to be adhered by analysts. An organisation is in need to identify its SOC scope as it is an essential aspect for it to work efficiently. The last category of SOC is technology which involves all the devices such as hardware and network components plus software that are in control of keeping the network safe and dealing with alerts and records .

One study [6] added that the percentage of assets monitored by organisations can be disappointing. Authors argued that in some firms SOC only monitor 5% of the systems. Also, the quality aspect seems to be absent where organisations are recommended to implement custom efficient use cases instead of relying on general basic monitoring. Some processes such as, events playbooks are meant to be added to SOC tools but in some cases, they might not exist or if they do exist, they are not updated. As well, the lack of SOC capacity and standardisation are associated with skills shortages in cyber security and organisations who have different understanding of SOC perceptions.

On the other hand, security approaches are part of SOC, but they can have limitations [7]. For instance, correctly configuring firewall can be difficult task to achieve. Therefore, users might face obstacles in performing internet-based activities until firewall is set up efficiently. Some systems can also face service slow down due to implemented security policies. SOC elements are required to continuously be managed and controlled for any upcoming updates. Services including data analysis via SOC aim to analyse network traffic to catch and prevent malicious activities as early as possible. Hence, these services must be applied correctly without impacting on the other sides of the business. Implementing the correct services is essential when constructing SOCs.

Another study [8] also mentioned that organisations are facing failure when inaccurate services are being applied. The lack of having a clear strategy is one of the main challenges that occur with SOC implementation. Threat monitoring, threat hunting and threat investigation are the suggested areas of focus. Covering these aspects helps in triggering meaningful alerts so analysts are able to understand and identify the required data. Establishing a strong architecture begin from the first stages where SOC team is suggested to gather and grasp the requirements effectively.

Therefore, study [9] revealed that SOC analysts raised concerns in regards to phishing attacks where employees are required to be trained efficiently in order to prevent such attacks. According to the study, a major phishing attack occurred in an organisation during the 30 days just after providing phishing training to employees. This indicates that inefficient training can be a problem.

Also study [5] on security operations centre at several organisation highlighted numerous challenges such as high false positive rates, the insufficient quality of threat intelligence and low quality of automation level.

Accordingly, SOC tools used by huge number of organisations could generate false positive alerts [10]. For example, cloud access security is one of these tools that produces alerts alongside other security monitoring devices. Therefore, some security analysts ignore alarms due to the high amount of false positive alerts.

But Mutemwa et al [4] stated that communications skills are the main key element when working with people from several department and roles. For example, when introducing SOC, a gap can occur where stakeholders of technologies and processes in an organisation might not understand the roles of cybersecurity team. Hence, the main reason of this gap can be misunderstanding and miscommunication amongst stakeholders and SOC team. Secondly, a variety of technologies can be found in an organisation but not all of them might be up to date. Some of them might be new or legacy. In this scenario SOC technology can be the latest versions of hardware or software and integrating it with an existing old technology can be challenging. In fact, several enterprises accept the risk of running existing legacy systems due to the cost of implementing new technologies.

The number of alerts, false positives, workloads, manual tasks and the complexity of attacks are amongst the most addressed challenges that SOC analysts face as study [11] reported. For example, Agyepong et al [11] pointed out examining or investigating every single alert is impossible and analysts are required to be supported with automation methods. Log management is a vital tool of SOC in analysing real-time traffic. Log data is described as a type of an event that keeps record of certain activities on an operating system, networks or any other appliances. Security Information and Event Management (SIEM) are the usual log management tools that complement SOC as an overall term. It is important to highlight that a log will contain information such as; date, time, users, type of operation and if it was successful or not. SIEMs are useful and assist holistically in optimising security posture due to investigations and reporting capabilities [12].

A lot of organisations are operating their SOCs by relying on SIEMs. They are identified as effective control tools that have the ability to automatically collect large set of events in real time environment and analyse them based on predefined rules [13]. One of the automation approaches can be applied by grouping similar alerts based on similar issues to support analysts in resolving the same issues more efficiently. Alerts that are part of the same source and are regenerated for the same reason can be classified into a specific alert sequence, which in turn can also be categorized into alert groups [14]. The reality is that automation processes are still not efficiently implemented as they sound, and it will take more time to be fully relied on as technologies change continuously. But automation also proved to be useful solution in supporting both skilled and less skilled analysts according to Crowley and Pescatore [15].

Additionally Dun et al [16] claimed that there is a gap in SOC sector and additional studies are recommended into the topic. Human, processes and technology components are all recognised in most of the literature that have been reviewed by previous authors, but operations and configuration were differently implemented in each investigated SOC model. The study showed that there are

disadvantages and lack of sufficient documentation for developing a SOC. Dun et al [16] suggested future research on SOC as there are still no proper guidelines that organisations follow to secure data and architect operations. It is also recommended to implement unique correlations rules for SIEM systems to model real time threats detection. Overall, the implementation of a productive SOC is determined by the correct integration amongst its components.

3 Methodology

3.1 Overview

In this section of the paper, we demonstrate our study approach and finding analysis. In fact, the design of the study is exploratory in nature. Our aim is to identify the key challenges that are being faced by SOC specialists in UK from an industrial point of view and link them to previous literature. Achieving this goal is completed by interviewing SOC experts from various types of firms including medium to large enterprises [17].

3.2 Participants

The individuals who are experts in the chosen field and who have experienced working within SOC were targeted. Unstructured interviews were carried out with five participants to gain the insights of challenges that are being faced in a SOC environment. All interviews were conducted online via Microsoft Teams to overcome geographical barriers, to facilitate interview recording, and as it was unlikely for the interviewer to be allowed to visit SOC environments physically. Only five interviews were conducted as it is challenging to identify SOC specialists who are willing to be interviewed or share data with regard to SOC challenges, largely due to confidentiality and data protection concerns. Also, the chosen number of participants help in narrowing the research focus on specific challenges and gain more details on them instead of having broad wide of information with limited depth.The role of the participants can be found in Table 1.

Table 1. Participants Information

Participant ID	Role	Interview Method
A	Cyber Security Engineer	MS Teams
B	Cyber Security Consultant	MS Teams
C	Cyber Security Architect	MS Teams
D	Head of Cyber Defense	MS Teams
E	Cyber Security Consultant	MS Teams

3.3 Ethics

Direct identifiers of individuals are removed to obey with confidentiality and ethics regulations. Reputation damage, employability loss or even criminal liability can be the result of such a disclosure of information that respondents can be affected by. Therefore, participants were able to stop responding to any questions if they had privacy or confidentiality concerns [18]. MS Teams is used to record the interviews and participants were given the choice to turn their camera on/off. The recordings were saved and only accessed by the researcher using password protected one drive account.

3.4 Data Collection Method

The reason behind choosing interviews as a data collection method is that it allows for accessing people's experiences and reality by asking follow up questions that were not thought of before the interview [19].

Questions such as ***'What is your role in Security Operations Centre?'*** and ***'How long you have been doing it for?'*** are asked but the nature of interviews was an informal conversation using an unstructured approach. Hence, participants had the chance to add any extra information that were not highlighted in questions where needed. These questions are important so the collected data can be analysed from different dimensions or demographers.

Accordingly, the nature of this research is associated with SOC which raise confidentiality and data protection issues. Hence, observations, experiments on organisations with SOC or collecting numerical data from organisations SOC tools was not possible due to these ethical concerns.

3.5 Analysis

Our data analysis is conducted using descriptive analysis and by presenting summary of the key challenges that were raised by the interviewees. A discussion is carried out to find any relationship between findings and previous conducted literature.

In fact, interviews were recorded and transcripts created. A coding approach was used to refer to each participant. Each participant mentioned specific challenges according to their role and organisation‘s size. Role specification and organisations size both influenced the challenges faced. For example, board level issues were only mentioned by participant D due to the role specification of this participant in being a point of contact with members of the board.

4 Findings and Challenges

The findings of the interviews were broken down into subsections to allow for a better understanding and clarification of the challenges faced. Nine main challenges were identified where each participant highlighted several challenges.

4.1 Number of logs

Participant A, a cyber security engineer that works for a security organisation, indicated that the massive amount of data logs is the key challenge that the industry is facing. For example, a small medium size company with up to 10000 computers could collect windows security logs, domain logs, and other logs from domain controller. For example, if the size of each log was a couple of megabytes, therefore the overall size would be the megabytes multiplied by 10000. Hence, the interviewee also mentioned about the importance of having an advanced infrastructure and automation to be able to deal with logs.

Meanwhile, the organisation of participant E was facing a huge number of false positives. To deal with it, they use what is called a 'continuous service improvement plan' where they look into fine tune and slim down the number of noisy alerts to try and pick the most valuable alert out of all these logs. The team could be dealing with up to 8 million alerts; therefore, they make sure that they work together following continuous service improvement (CSI) process to reduce that noise. When asked about any planned solutions or suggestions to overcome this difficulty participant E provided the following example. They had a client that use Splunk as SIEM.

Splunk is one of the well-known SOCs SIEM tools, it consists of three main elements: Search bar, Indexer and Forwarder. Each component has its own role to deliver a comprehensive SOC solution. The indexer is utilised for storing and processing the generated logs to help in analysing the data and search for particular logs when needed. Splunk also has its own language when searching for events, it is defined as Splunk Processing Language (SPL) similar to SQL queries a user is required to type the queries into the search bar in order to retrieve the required information which can be provided in various formats such as reports, charts or even on dashboards. The final component is forwarders where logs are being collected and forwarded to indexers [20].

Thus, the client also used Splunk phantom playbooks on top of it which helped massively in decreasing the number of false positive logs. It works by being able to whitelist an IP and to automatically filter through the whole scene tool, then it would be automated out. As a user/analyst you will not be required to try triage that particular incident anymore. All it takes is to just whitelist it and be added to the system, hence this level of automation can reduce the noise. The interviewee insisted on the automation as it is the future of a SOC in order to reduce the number of manual efforts.

4.2 False Positives

The high number of events and alerts pose a major challenge amongst trying to pull data from external sources using threat intelligence. An example is provided by interviewee C, where an event occurred such as false positive, and a good

number of analysts started investigating the issue. Then, the event turned out to be badly scaled and misunderstood where it was a one-person job, and it could‘ve been dealt with easily. As stated, if a genuine threat has occurred at the same time where other people were investigating the fake event, the risks could‘ve been high.

Adding to the above, the previous role of interviewee D revealed that 95% of the defined incidents were ultimately false positive as participant stated. In the current role environment, the ratio is reduced to be 50% of false positive alerts. It is a big challenge as analysts are unable to go far beyond that without having in depth machine learning tools. A risk can be run where true positives could be lost whilst investigating false positive ones. It is a disturbing situation where analysts are required to spend time in the right places where losing a true positive alert can lead to a disaster the head of cyber defence emphasised. On reflection in terms of probability this may result in a lot of false positives, or an alerting logic may result in a lot of false positives.

Thus, if it‘s 95% at the time it‘s false positives then there are few essential questions that need to be raised. Would the company just take the risk of giving 12 hours’ worth of analyst time back to the SOC? and who could be looking at other threats? So, it is vital for the business to identify wither an alert was true or false. As D added in the current workplace it‘s balanced with 50/50 ratio but they are trying to reduce it as much as possible. They rely on experienced analysts when dealing with false positives where they can get into a conclusion once a ticket is open due to their in-depth knowledge and familiarity working experience with the network and its behaviours. But this can also lead to a triage biasing, and it is a tricky situation to reduce the number when relying on manual investigations.

4.3 Lack of Communication

On the other hand, interviewee B added that communication amongst analysts is one of the biggest challenges that SOC users face. For example, analysts spent 12 hours a day working in SOC where they get burnt out at the end of the shift. Hence, there is no time to speak about things, and also, some of the analysts are new to SOCs. There are also false positive logs but with better communication amongst team members finding out false positives can be detected a lot easier. **Geographic challenges** are also added by participant C in terms of communication. Analysts are often working remotely where they occasionally go to the office. Therefore, communications amongst analysts can cause a challenge more specifically when also trying to speak to the national cyber security and national crime agency as they added.

In fact, it is important to communicate with NCSC. One of the effective services they provide is called Cyber Security Information Sharing Partnership (CISP) for UK organisations that are bounded by cyber security. Only registered

UK organisations and government are able to share cyber security threats information amongst themselves in a protected and private environment. Storing, correlating and managing threat intelligence is achieved via Threat Intelligence Platform (TIP). The platform enables automation for detecting Indicators of Compromise (IoC) by connecting to the SIEM tool. There are various types of TIPs, and it depends on whether an organisation is using commercial tools or not. Implementing threat platform is beneficial to increase the SOC value by feeding it with a wide range of intelligence [21].

Participant D added that communications amongst analysts is effective to share important information and knowledge. It can be a struggle specially where they monitor and investigate the network between 12-13 hours a day. At the meantime this has been improved as they have been encouraged to conduct training and learning. For instance, senior members of SOC are usually pair up with either graduates or new analysts of the SOC team. Therefore, when unusual activities are occurred and they have never experienced it before, then senior staff can elaborate further on that as "D" has explained.

4.4 Lack of Skilled Analysts

Other challenges are mentioned by interviewee A in terms of analysts, where if an experienced staff leaves then a new analyst joins it would take a lot of time for them to gain the skills required for the job. This issue might occur continually where it puts the employer back to the first step, hence a rigid training regime is required.

Participant A emphasised on the challenge as stated:

"It's a losing battle because data is increasing. There's already a shortage of cybersecurity workers, and inside of that shortage, there's a shortage of analysts. It's a moving target to hit, whereas data is increasing, you still need to retain and not just retain. You can't just retain; you have to increase your overall head count of analysts".

When asked interviewee E about the main challenges that they currently face, the consultant added that one of the most significant issues is the quality of events. This means that when an event is being triaged to level 3, they require to look into it in a detailed investigation where it consumes time and effort. Hence, the quality of it is needed to be as high as possible to reduce workload on tier 3 analysts. The biggest gap at the meantime is the skill difference from level 2 to level 3.

Accordingly, there is another challenge which is the rotating door at tiers 1 and 2 analysts. Building a relationship with the company who is responsible of that is quite difficult due the rotating of analysts where analysts at that level might be moved around into different projects which makes it harder to start again with new analysts. As a result, communications gaps can be clearly

noticed and recognised. As part of the services that participant E company offer outsourced SOCs products. Thus, their current client level 1 and 2 analysts are being provided by external partner but sometimes E can be on the opposite side while their firm is the one that provide tier 1 and 2 services. Therefore, almost every member of the team agrees on the same issue of communication amongst each other where partners and the rotating analyst expose challenges to communication layer.

4.5 Unexpected Users Behaviours

The other side level of the challenges comprises users' behaviours and activities on the network. Therefore, the organisation that participant D work for spend a huge amount of money up to £10 million per year to enhance their monitoring tools and security controls for particular packages. But threat actors are still able to jump over these measures due to users' behaviours where phishing is a good example of this. Thus, organisations are always under the risk of potential ransomware attack due to their users clicking on malicious link received via scam emails. It can be highlighted that the biggest struggle for the organisation is users' activities where no matter how many controls they apply into the place a user will still cost them and then the mentioned £10 million of security controls can be relatively ineffective because of one user‘s behaviour.

The following is also stated by D:

"It's a continual thing where it has to be recurring themes. The forefront of their mind and to keep them out of those sorts of behaviours. It's that balance between being too much where people switch off because they're being bombarded with information or it's not relevant to what they're doing. We do some very basic things, so yeah, I think one of those key things is definitely around awareness."

From a security point of view, the biggest challenge is phishing attacks, where it is quite hard to detect them when they occur. According to participant B it is very difficult to try and stop these types of attacks apart from reporting them when they are detected. When it comes to phishing attacks, team members agree on this challenge but not only within SOCs, also within the whole cyber security sector. Following on from that, sometimes users who have less technical skills and do not work in a SOC do not admit that they clicked on a phishing link because they are not sure about the consequences, so they prefer to be quiet. When asked about any planned solutions to overcome these challenges, B mentioned that in Microsoft office 365 there is a report phishing function but when it comes to looking at logs and try to report these logs in a certain process, there is still a lot of work that needs to be done. However, there is no %100 solution where it says that this is definitely how we are going to stop phishing attacks. However, cyber security industry is constantly moving forward, and it is still quite difficult to stop phishing.

4.6 Lack of Automation

Participants C,D and E agreed on the lack of automation when working with SOC. For instance, C mentioned that having some sort of automation in place to reduce the workload would be an effective solution. Participant also added that events correlations are required to have some kind of automation that can pull data from external sources and partners for threat intelligence using particular algorithms. On the other hand, when asked interviewee D about the role of machine learning and implementing automation techniques to try and mitigate false positives where analysts can have more focus on real true ones. The answer was the following:

"Yeah, absolutely I mean, ultimately, it's all data right so even false positives. That data and they've got something that alerts you to the fact that they're false positive so one thing I've looked at in the past with machine learning is to take all those false positives because usually they are a consequence of something happening on the network."

4.7 Variety of Solutions

A stuck between two various solutions are the technical challenges that participant C organisation face. For instance, the organisation has different departments in various areas where some use specific tools and some use different ones. Therefore, combing both solutions into one main is a challenge for them. Analysing the output of both solutions into one main base like having a coherent repository that store the data for analysis can be a solution.

4.8 Gap in Threat Intelligence and Manual Actions

According to participant C threat intelligence is heavily relied on manual actions. There are up to 6 individuals who are based in office searching for information to keep track of trends. For instance, windows services threats related information are pulled out manually. Having some sort of 20-30% of automation or even more is useful to pull these types of data where workers can focus on dealing with other tasks. Threat intelligence is a massive gap at the moment in terms of what information or threats to look for and automation can reduce the manual work. Mapping the monitored systems and spotting gaps can enhance our work effectively and efficiently as participant C concluded.

4.9 Board Level Issues

Stakeholders and individuals who are part of the board do not necessary recognise the risks that are associated with cyber security. For example, it can be quite challenging for them realise and understand the real impact of such a cyber-attack unless they experience a genuine threat/attack. Accordingly, this

might be due to the lack of education and awareness of cyber security as D added. On the other hand, investments can reach into an end road. This means that money is put towards solving of such a gap but when it is resolved the funds stop where new threats might occur. Various organisations and boards are still under the belief that they can win when a solution is achieved, they the move on. The real environment of cyber security is about continuity and improvements, it's not about solving an issue and move on participant stated. Currently, a good number of board members understand and realise the need of ongoing investments, but there are still a lot of facts to be shared with them in order to appreciate the changing culture of cyber security.

4.10 Conclusion

To conclude the identified challenges, table 2 below summarises the nine challenges faced by each participant. A-E codes present each participant. To avoid duplication of challenges the researcher decided to add (X) next to each challenge that is mentioned by each participant. For example, number of logs is only added by participants A and E. Thus, the following section will discuss and analyse findings more in-depth.

5 Discussion and Analysis

Table 2. Challenges Faced By Security Operations Centre

Challenge	**A**	**B**	**C**	**D**	**E**	**Total**
Number of Logs	x				x	2
False Positives			x	x	x	3
Lack of Communication		x	x	x		3
Skilled Analysts	x	x			x	3
Users Behaviours		x		x		2
Lack of Automation			x	x	x	3
Variety of Solutions			x			1
Threat Intelligence			x			1
Board Level Issues				x		1
Total Challenges Faced	2	3	5	5	4	

This section highlights the findings of the conducted study to discuss the connection between the gathered data and the literature review associated with SOC challenges. The above table illustrates the key challenges that have been highlighted by interviewees. The first column contains these challenges whilst letters A-E refer to participants IDs. The author added "X" next to any challenge that have been identified by specific individual.

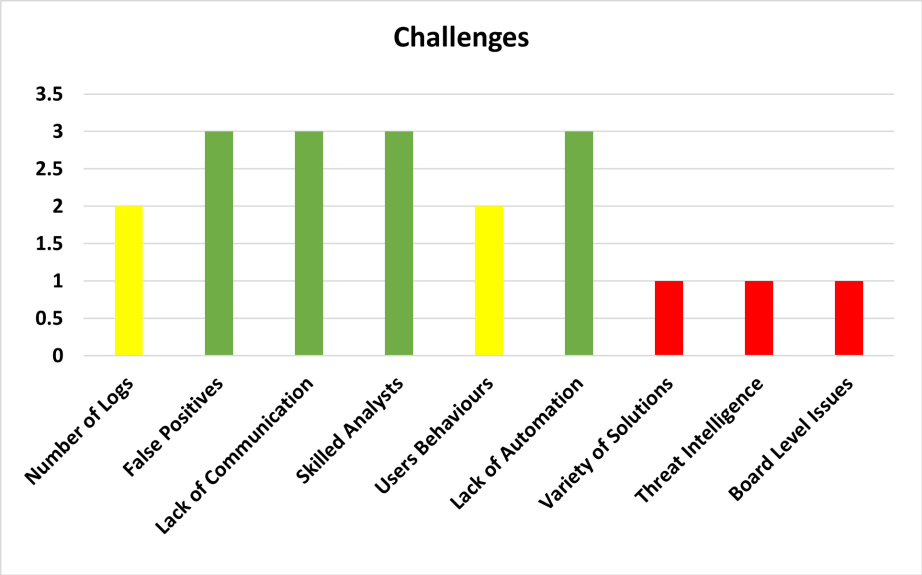

Fig. 1. Challenges Faced by SOC Analysts

Accordingly, the identified challenges are 9. Therefore, table 2 provides calculation of each identified one. For instance, false positives, lack of automation, lack of communication and skilled analysts are mentioned 3 times amongst participants. Hence, they are the most common amongst the gathered insights. Figure 1 is an illustration of the number of the mentioned challenges as it depicts the highest and lowest challenges mentioned by participants.

In fact, in terms of the mentioned and faced challenges there are differences between participants due to various aspects such as the size of the organisation and roles of individuals. Figure 2 depicts the number of challenges faced by each participants.

One of the observations when it comes to the number of challenges mentioned by each participant. There seems to be a relationship between the role of participant and the number of challenges. For example, the role of participant D is head of cyber defense which is higher than other roles. Thus, the number of challenges mentioned by D is 5. In contrast, participant A is a cyber security engineer which is less responsibilities than head of defence. Hence, the challenges raised are only 2. As a result, the higher the position is the more challenges are being faced.

In addition, Onwubiko and Ouazzane [6] highlighted the lack of SOC standardisation and understanding due to skills shortages in SOC. Participants A B and E also emphasised on the big gap when it comes to skilled analysts shortages.

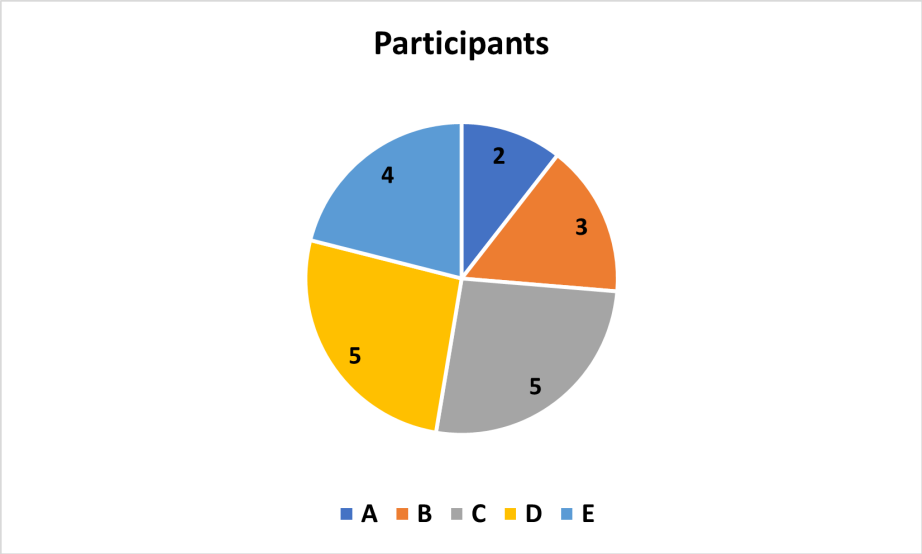

Fig. 2. Participants Chart

Another raised concern is with SOC services or polices that can impact on services efficiencies by slowing down the speed as mentioned by Nalanagula and Roy [7]. This can be related to the variety of solutions implication that is mentioned by participant C where combining various tools and services into a main one could be beneficial.

Also, implementing the correct services is essential as added by Bikov et al [8] but this could lead to conflict decision between SOC manager and stakeholders which is part of the board level issues identified challenge by participant D.

Ban et al [10] mentioned that a lot of tools could generate false positive alerts but turning off one of these services could expose systems to major risks which is an implication added by participants A and E in terms of the number of generated logs.

Alharbi [5] raised a concern in terms of the quality of automation and false positives. Lack of automation and the number of false positives seem to be an issue amongst most of organisations. Participant D added that automation and machine learning can help in working through specific patterns where an analyst would be able to pick out outliers that they do not fit with false positive patterns.

Accordingly, users' behaviours challenge is also raised by Kokulu et al [9] in terms of having efficient training to prevent attacks such as phishing ones which can cause overwhelming job on SOC analysts. To try and reduce the impact of the users' behaviours, "D" mentioned that cyber awareness module training is

required to be taken by all company users, but they spend up to 20 minutes working on it and they just forget about it.

Additionally, Mutemwa et al [4] stated that communications skills are key when working with people from different departments such as cyber security team and internal IT team. Most of the participants mentioned the importance of communication amongst analysts where it can be challenging due to the amount of time they need to spend on investigation and analysis of security events.

6 Conclusion and Future Work

Referring back to the research question ***'What are the main challenges faced by SOC analysts and how they impact on orgnisations?'*** the purpose of this paper was to assess the challenges that has been mentioned in previous literature and by interviews with those in SOCs. This has contributed to the field of research by gaining new insights from targeted individuals. This paper has identified nine key challenges from an industry perspective. The literature review supported the study from an academic point of view by also highlighting the challenges of SOC identified by previous authors and linking them to the outcomes of the interviews.

Future research can focus on proposing a model to overcome these challenges. A solution could be implemented separately to each one of the identified challenges or an overall solution for all of them. More precisely, implementing a framework that can be utilised by organisations will be the intended future work of the author to overcome the identified challenges. An evaluation will be collected from the interviewed individuals with regard to the framework to identify its weaknesses where continuous improvements can be applied.

Also, technical work will be carried out in terms of automation to implement a solution that can mitigate noise from false positives or false negatives. As part of the automation, machine learning approaches can be suggested and implemented by carrying out experiments to tackle some of the identified challenges. Accordingly, the research can be expanded further to conduct interviews with SOC specialists around the globe and discover if there is any additional or similar challenges to those faced by SOC specialists in the UK.

References

1. M. A. Majid and K. A. Z. Ariffi, "Success factors for cyber security operation center (soc) establishment." EAI, 10 2019.
2. T. H. Nguyen, "Cybersecurity logging & monitoring security program," *School of Computer Science Engineering, Sacred Heart University*, pp. 1–8, 2022.
3. M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020.

4. M. Mutemwa, J. Mtsweni, and L. Zimba, "Integrating a security operations centre with an organization's existing procedures, policies and information technology systems," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 2018, pp. 1–6.
5. S. A. Alharbi, "A qualitative study on security operations centers in saudi arabia: challenges and research directions," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 24, 2020.
6. C. Onwubiko and K. Ouazzane, "Challenges towards building an effective cyber security operations centre," *International Journal on Cyber Situational Awareness*, vol. 4, no. 1, pp. 11–39, dec 2019. [Online]. Available: https://doi.org/10.22619\%2Fijcsa.2019.100124
7. S. Nalanagula and A. Roy, "Cyber security operations centre: A user-cantered machine learning framework."
8. T. Bikov, D. Radev, T. Iliev, and D. Stankovski, "Threat hunting as cyber security baseline in the next-generation security operations center," in *2021 29th Telecommunications Forum (TELFOR)*, 2021, pp. 1–4.
9. F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched socs: A qualitative study on security operations center issues," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1955–1970. [Online]. Available: https://doi.org/10.1145/3319535.3354239
10. T. Ban, N. Samuel, T. Takahashi, and D. Inoue, "Combat security alert fatigue with ai-assisted techniques," in *Cyber Security Experimentation and Test Workshop*, ser. CSET '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 9–16. [Online]. Available: https://doi.org/10.1145/3474718.3474723
11. E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Challenges and performance metrics for security operations center analysts: a systematic review," *Journal of Cyber Security Technology*, vol. 4, no. 3, pp. 125–152, 2020. [Online]. Available: https://doi.org/10.1080/23742917.2019.1698178
12. T. Eskelinen, "Development of open-source siem and security operation centre in a company," *South-Eastern Finland University of Applied Sciences*, pp. 1–46, 2022.
13. J.-y. Kim and H.-Y. Kwon, "Threat classification model for security information event management focusing on model efficiency," *Computers & Security*, vol. 120, p. 102789, 2022.
14. C. Engel, S. Mencke, R. Heumüller, R. Hormann, H. Aedtner, and F. Ortmeier, "Customizable operation center for smart security management," *Procedia CIRP*, vol. 104, pp. 1930–1935, 2021, 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827121012245
15. C. Crowley and J. Pescatore, "Common and best practices for security operations centers: Results of the 2019 soc survey," *SANS, Bethesda, MD, USA, Tech. Rep*, 2019.
16. Y. T. Dun, M. F. Ab Razak, M. F. Zolkiplib, T. F. Bee, and A. Firdaus, "Grasp on next generation security operation centre (ngsoc): Comparative study," *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 869–895, 2021.
17. M. Saunders, P. Lewis, and A. Thornhill, "Study methods for business students," pp. 128–140, 2019.
18. E. Singer and M. Couper, "Ethical considerations in internet surveys 1," *Social and Behavioral Research and the Internet*, pp. 133–162, 2018.

19. Y. Zhang and B. M. Wildemuth, "Unstructured interviews," *Applications of social research methods to questions in information and library science*, pp. 222–231, 2009.
20. M. Hristov, M. Nenova, G. Iliev, and D. Avresky, "Integration of splunk enterprise siem for ddos attack detection in iot," in *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, 2021, pp. 1–5.
21. "Building a security operations centre (soc)," https://www.ncsc.gov.uk/collection/building-a-security-operations-centre, accessed: 2022-06-04.