Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues

Faris Bugra Kokulu
fkokulu@asu.edu
Arizona State University

Ananta Soneji
asoneji@asu.edu
Arizona State University

Tiffany Bao
tbao@asu.edu
Arizona State University

Yan Shoshitaishvili
yans@asu.edu
Arizona State University

Ziming Zhao
zxzics@rit.edu
Rochester Institute of Technology

Adam Doupé
doupe@asu.edu
Arizona State University

Gail-Joon Ahn
gahn@asu.edu
Arizona State University and
Samsung Research

ABSTRACT

Organizations, such as companies and governments, created Security Operations Centers (SOCs) to defend against computer security attacks. SOCs are central defense groups that focus on security incident management with capabilities such as monitoring, preventing, responding, and reporting. They are one of the most critical defense components of a modern organization's defense.

Despite their critical importance to organizations, and the high frequency of reported security incidents, only a few research studies focus on problems specific to SOCs. In this study, to understand and identify the issues of SOCs, we conducted 18 semi-structured interviews with SOC analysts and managers who work for organizations from different industry sectors. Through our analysis of the interview data, we identified technical and non-technical issues that exist in SOC. Moreover, we found inherent disagreements between SOC managers and their analysts that, if not addressed, could entail a risk to SOC efficiency and effectiveness. We distill these issues into takeaways that apply both to future academic research and to SOC management. We believe that research should focus on improving the efficiency and effectiveness of SOCs.

KEYWORDS

Human factors; Security Operations Center; interviews

ACM Reference Format:
Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. 2019. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3319535.3354239

CCS '19, November 11–15, 2019, London, United Kingdom
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6747-9/19/11…$15.00
https://doi.org/10.1145/3319535.3354239

1 INTRODUCTION

Computer security attacks are a significant threat to our society. Organizations suffer frequent attacks by highly sophisticated and systematic adversaries with different agendas, and these attacks, if successful, result in severe consequences to the organizations, their clients, and their partners.

Many organizations have created *Security Operations Centers* (SOCs), generally in the form of a centralized group composed of security specialists who monitor, prevent, report, and respond to security attacks. While such SOCs have been shown to help improve companies' security posture [22, 28, 39], serious security incidents remain rampant [40], and the current SOC setup is insufficient to defend against these attacks.

The reasons why SOCs fail are complicated; representing a mix of technical and human-centric issues. For example, in 2013, attackers managed to breach Target's network and steal their data, despite Target following "industry best practices" by deploying a $1.6 million malware detection tool and enforcing "reasonable security controls in place" [37]. Before this incident occurred, Target's subsidiary SOC had successfully detected the issue and reported it to the main SOC. However, for unknown reasons, the main SOC did not take further action beyond the detection. As a result, the data breach issue persisted and caused significant losses.

To improve the effectiveness and efficiency of SOCs, it is imperative for the security community to identify problems facing SOCs and create solutions to fortify these critical components against the ever-growing number of attacks. Unfortunately, little research has been done to investigate the issues faced by SOCs. Previous work focused on analyst efficiency [2] and burnout [43] in SOCs, but there is a lack of research that *comprehensively* studies *what* issues exist in SOCs. This shortage renders the academic community unaware of practical problems and struggles that SOCs must contend with, leaving them ill-positioned to address these significant challenges.

In this paper, we conduct a qualitative study to discover the issues of SOCs. In contrast to quantitative research, qualitative research focuses on *meanings, concepts definitions, characteristics, metaphors, symbols, and descriptions of things* [29], which is aligned with our goal of studying *what* the issues are in current SOCs.

This research is based upon a one-year study with a total of 42,895-word transcripts of interviews with security practitioners in various SOCs. In this study, we invited 57 SOC employees—both managers and analysts—across 46 companies to participate, and 18 of them agreed to participate in a 45-minute in-depth interview to discuss their understanding and concern of their SOC. We audio-recorded, transcribed, anonymized, and analyzed all the interviews by applying the iterative open coding approach [42].

We analyze the issues that analysts and managers reported and, interestingly, found both agreements and contradictions among them. In our analysis, we highlight the research problems that the academic community should address to benefit SOCs in dealing with real-world security threats. Based on the study, we have key findings as follows:

Low visibility into the network infrastructure and endpoints is the *most* common issue in SOCs. Among all of the issues that SOC operators identified (Section 2), low visibility into the network infrastructure and endpoints is the most acknowledged issue that prevents SOCs from being effective. The participants reported that low visibility is their biggest concern in security operations (Section 4.1.1).

Phishing attacks are the most common attacks faced by SOCs, yet current phishing defense training provides little help in resolving the issue. In the interviews, 15 out of 18 participants mentioned that phishing the attack experienced most often. One possible way to prevent phishing attacks is to educate employees to be alert of suspicious emails. However, we found that such education is not as effective as we expect in practice. In particular, one participant mentioned his experience where a severe phishing attack took place on an employee within 30 days after the phishing defense training (Section 4.1.2).

False positives in malicious activity detection *do not* majorly impact SOC operations. Five interviewees reflected their significant concerns regarding having a large volume of unfiltered, unrelated, and uncorrelated alert data (Section 4.1.3). Moreover, reports and logs that are automatically generated by SOC systems may contain inaccurate or ambiguous information, which affects SOC performance (Section 4.1.4). However, *none* of the interviewees consider false positives in automatic malicious activity detection as a *major issue* in SOC operations, which is in opposition to academia's belief that false positives are fatal in automatic detection (Section 4.1.5).

Current SOC performance evaluation metrics are ineffective in measuring SOC success. Current quantitative metrics, such as the number of incidents and average response time, are not effective in measuring SOC success because each security event has unique severity and consequences (Section 4.2.2).

Speed of response and level of automation, evaluation metrics, and tool functionality are the top three controversial issues between analysts and managers. Through our qualitative analysis of our interview data, we discovered inherent disagreements between managers and analysts regarding issues facing their SOC (Section 4.2). Analysts and managers have conflicted and mismatched perspectives toward these issues.

Based on our findings, we provide actionable advice for SOC professionals to help them improve the effectiveness and efficiency of their organization's SOC. Furthermore, we derive research opportunities for the academic research community to help them recognize the real-world concerns and needs of SOCs.

2 BACKGROUND

A Security Operations Center (SOC) is a group dedicated to preventing, detecting, and responding to the security incidents in an organization. In contrast to Network Operation Centers that operate and maintain the network equipment, or physical security departments that are responsible for physical surveillance and security of organizations, a SOC is responsible for monitoring, assessing, and defending an organization's computing environment by using a collection of tools, technologies, and processes. A SOC may have a different name, such as Cyber Security Operations Center (CSOC), Computer Security Incident Response Team (CSIRT), and Information Security Operations Center (ISOC) [55]. In this paper, we will refer to all such defense groups as SOCs.

Managers and analysts within a SOC collaborate to mitigate the security threats in an organization. An organization typically consists of networks, servers, databases, websites, applications, and endpoints. A SOC analyzes activity over all the different units in the organizational architecture to identify compromises.

Organization Resources. In this study, we consider two types of SOCs: internal and outsourced. An *internal SOC* is part of the organization they defend: it is operated and managed internally by the organization. An *outsourced SOC* is an independent party which an organization pays for SOC services. These SOCs are operated and managed by an independent party, and typically report to a designated entity who is a member of their client's organization.

Human Hierarchy. One of the major tasks of a SOC is to consume and analyze incident-relevant data. These incidents are events observed on the company network and its endpoints, which may require further actions. A SOC collects, analyzes, and stores very large volumes of data daily from logging mechanisms. For instance, intrusion detection systems, which generate logs, are placed on the network to capture potentially malicious activities and to provide information regarding that activity to SOC analysts. SOCs dedicate a group of individuals that perform real-time triage of these received alerts, logs, and events on their network.

This group of system analysts is called *Tier 1*. Some of the additional responsibilities of Tier 1 analysts include real-time monitoring and configuring system tools. They perform the initial investigation of the incident, and if the incident is out of the scope of their responsibility or if their skill-set is not enough to investigate that incident, they escalate it to the next tier (the *Tier 2* analysts).

The Tier 2 analysts perform an in-depth analysis of the incident. They review the Tier 1 analyst's reports to identify affected systems and the scope of the attack. Based on the collected evidence, Tier 2 analysts take actions such as blocking an activity, deactivating an account, watching the network for further evidence, or escalating the case to a higher-tier.

In general, as the tier level increases, the responsibilities of the analysts become more specific. Moreover, the time expectancy of solving incidents of each tier tends to differ, where analysts from a lower-tier are expected to resolve incidents faster than a higher-tier, as incidents that escalate are more complex.

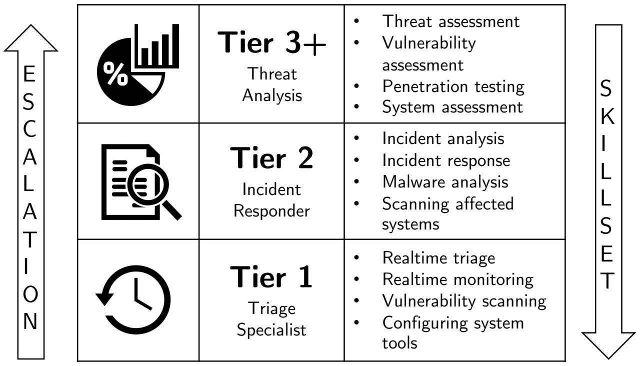

Figure 1: Typical SOC analyst tier responsibilities [55].

In large organizations, there may be other tiers that perform tasks such as threat hunting, vulnerability assessment, and penetration testing. Broadly, these tier layers are called *Tier 3+*. A graphical representation of the tiers with their responsibilities is shown in Figure 1. It is important to note that not all SOC have such a hierarchical structure. In non-hierarchical arrangements, all employees are expected to have similar skill-sets which makes them capable of handling incidents individually.

3 METHODOLOGY

We conducted 18 semi-structured interviews with SOC analysts and managers from six different industry sectors: airline, construction, education, financial services, information technology, and professional services. The interview questions cover topics such as the SOC types, the hierarchical structures, the technical and managerial operations, and the evaluation metrics. For the details of the interview questions, please refer to Appendix A. To have exhaustive results, we did not stop conducting interviews until new themes stopped emerging from the iterative open coding procedure performed on the transcribed interviews [17].

Our study was exempted by our Institutional Review Board (IRB), as our questions did not measure individual behaviors. Despite this, we still followed the same ethics and privacy requirements that an IRB would normally enforce. When we transcribed the interviews, we anonymized the participant's name, the organization's name, and all personally identifiable information. The audio records of the interviews are kept encrypted.

Participant Recruitment. We recruited participants in two steps. In the first step, we contacted SOC-related individuals from various industry sectors through multiple vectors including searching profiles on LinkedIn, attending online security related business webinars, attending industry security events and conferences across the U.S., and asking known contacts. We sent each of these individuals an email with details about our research study, interview procedure, the motivation behind the research study, information regarding the data anonymization process, and potential benefits to the participants and their organizations. Unfortunately, only those in our known contact list replied to our request, and some of them agreed to participate. Throughout our search for potential participants, we recruited ten of our participants through emails and two of our participants at industry security events and conferences.

Participant ID	Position	Organization Resources
$P1$	Analyst	Internal
$P2$	Manager	Internal
$P3$	Analyst	Internal
$P4$	Analyst	Internal
$P5$	Manager	Outsourced
$P6$	Analyst	Outsourced
$P7$	Analyst	Internal
$P8$	Manager	Internal
$P9$	Analyst	Internal
$P10$	Manager	Internal
$P11$	Manager	Internal
$P12$	Analyst	Internal
$P13$	Manager	Internal
$P14$	Manager	Internal
$P15$	Manager	Internal
$P16$	Manager	Outsourced
$P17$	Analyst	Outsourced
$P18$	Manager	Outsourced

Table 1: Participants in our research study.

In the second step, to recruit the corresponding SOC manager/-analyst from the same organization, we used the Snowball Sampling technique, which is used to recruit future subjects by referrals from existing subjects [6]. We asked each participant to ask if their manager or their analyst would be interested in participating in our research study. In this way, we recruited an additional six participants.

As shown in Table 1, we recruited 5 participants who work in an *outsourced* SOC and 13 participants who work in internal SOCs. Due to ethical considerations, we do not provide any identifiers that would potentially reveal manager/analyst pairs who work in the same organization, including their corresponding industry sectors.

Interview Question Design. Our interviews included questions that were specific to roles. On specific topics, we designed questions that were only asked to managers. We selected these topics by considering role-specific authorizations and responsibilities. For example, we asked questions about integrating new technologies to managers because, typically, a manager can decide to add new technology to the SOC. Similarly, SOC budget is typically controlled by an entity who is situated either the equivalent of or higher than a manager in the organizational hierarchy. Because of this reason, we asked questions that are related to budget to managers. Regarding automation, we designed questions for analysts. We wanted to understand if analysts were allowed to automate their systems and their opinion on automation.

At the start of each interview, the interviewer mentioned that all questions were optional, and participants were free not to respond to any of them. It is worth noting that the interviewer did not ask questions in the order they appear in the Appendix A; the discussion flow with the participant determined the order of the questions and the interviewer had discretion to follow leads [4].

Data Analysis. We adopted the iterative open coding procedure [42] to analyze our interview data thoroughly. Two independent coders coded all interviews to ensure unbiased results. The primary researcher conducted and transcribed the interviews.

After finalizing the interviews and the transcriptions, the primary researcher created a codebook by coding the transcripts. Once the codebook was complete, the second coder joined the research

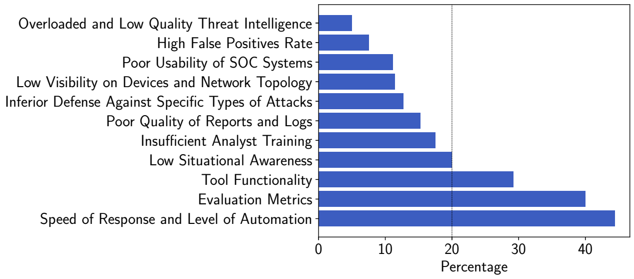

Figure 2: Issues identified through our qualitative interviews that had significant disagreement between analysts and managers. The percentage gap (x-axis) is the percentage of disagreement between analysts and managers (higher indicated higher disagreement). Issues are sorted based on size of percentage disagreement.

study. Both coders had similar backgrounds, with only the primary researcher having previous SOC knowledge. The primary researcher guided the second coder, in concepts of qualitative research studies and related methodologies, techniques for coding interviews, and SOC knowledge.

After the coding procedure, we calculated the Cohen's Kappa coefficient as a representative of inter-coder reliability score. The Cohen's Kappa coefficient for this study is 0.71, which Landis et al. [30] stated as a substantial score of agreement for categorical data.

4 SOC ISSUES

In this section, we discuss SOC issues that we uncovered from the interviews. Recall from Section 3 that questions such as budget plan and technique deployment strategy are manager-only due to the scope of work. For the issues from the questions answered by both analysts and managers, we calculate the respective ratiosof the participants agree with the issue, and we compare the ratios between analysts and managers, as shown in Table 2. We also sort the issues by the difference of the agreement between analysts and managers. Based on the sorted results, shown in Figure 2, we observe a gap in the analyst-manager difference of agreement: while most of the issues are under 20% difference, three of them are around 30% or above. In this paper, we call the issues with less than 20% difference the *matched issues*, whereas the ones with greater than 30% difference the *mismatched issues*. We will introduce the two types of issues separately, followed by the other issues identified by manager-only or interviewee-specific questions.

4.1 Matched Issues

Here, we discuss the issues that our participants have the most agreement. We selected them by observing the gap in the analyst-manager difference of agreement, shown in Figure 2.

4.1.1 Low Visibility on Devices and Network Topology

The lack of network visibility is the most common issue in our participant's SOCs: 71.43% of analysts and 60% of the managers, including both outsourced and internal SOCs, raised the concern that they were not able to learn the complete network setup and thus cannot enforce security operations effectively.

Network information helps a SOC to understand an organization's security posture and respond to security incidents. The information is of different types, such as "network architecture documentation," "list of devices in network zone models" (P18), "full asset inventory," and "configuration management database" (P5).

For example, P18 stated that the situational awareness (SA) (Section 4.1.7) is impacted by the level of visibility:

> *In terms of the clients that we have on board, our situational awareness is confined to the devices that are on board. We had several cases that they were sending alerts from devices that we never agreed to receive events from.*

In addition, P5 highlighted the impact of the incompleteness of network visibility on response speed:

> *We do not have a full asset inventory, that is a big constraint (for fast response). We do not have configuration management database, that is a big constraint (for fast response).*

The reason for incomplete network visibility is multi-faceted. Internally, the issue may be due to the structural setup of SOCs. For example, a tiered SOC with a hierarchical setup that is assigned limited visibility of incidents and machines to analysts at different tiers, described by P3:

> *SOCs that are tiered will have limited visibility based on its tier because a SOC analyst can accidentally make a mistake during escalation.*

Externally, incompleteness may be caused by the improper management or operation from another department. In specific, P18 mentioned the lack of information maintenance and the lack of the communication between IT operations and security teams:

> *(The information the SOC requests) is not always up to date. [...] (The SOC's receiving alerts from unknown devices) is usually because the IT ops and security teams are not necessarily the same people and messages get lost and things like that.*

P7 stated that visibility is impacted because of the administrators breaking organizational rules. In this case, the SOC monitors a large network that is connected to smaller sub-networks controlled by different administrators, and P7 observed scenarios where administrators decide not to follow pre-determined organizational guidelines in creating their infrastructure or do not report new devices that they connect to the network, which negatively impacts the overall visibility of the SOC.

P4 also complained about the company employees' disobeying the rules:

> *The company as a whole push for stronger device management and identification but it is a very difficult thing at a global scale. Sometimes, somebody does not necessarily bound to the same standards so they will just throw some routers to get the networks working.*

Also, the incompleteness is due to the nature of the organization, which requires flexibility of device connectivity. For example, P*[1] works for a particular sector with special requirements which makes it impossible to have high visibility all the time, given the fact that

[1] Our study includes a limited number of industry sectors, and this quote contains one of those sectors. Therefore, we anonymized our participant's ID to protect their identity against the possibility of de-anonymization.

Category	Subcategory	Analysts	Managers
Operational Issues	Low Visibility on Devices and Network Topology	71.43	60.00
	Inferior Defense Against Specific Types of Attacks	42.86	55.56
	Slow Response Speed of the SOC	20.00	50.00
	Inefficient Evaluation Metrics	50.00	10.00
	Insufficient Budget	—	44.44
Technological Issues	Overloaded and Low Quality Threat Intelligence	25.00	30.00
	Poor Quality of Reports and Logs	37.50	22.22
	High False Positives Rate	12.50	20.00
	Malfunctioning of SOC Tools	37.50	66.67
	Insufficient Automation Level of SOC Components	33.33	77.78
	Poor Usability of SOC Systems	33.33	44.44
	Challenge of Scaling SOC Technologies	—	30.00
Human Knowledge Issues	Low Situational Awareness	0.00	20.00
	Insufficient Analyst Training	37.50	20.00

Table 2: Heatmap of the percentage of SOC managers and analysts that indicated a specific issue in their interviews. We calculated respective ratios based on the total number of participants that answered each of our interview questions. This number varies for each category because all interviews were semi-structured. Analyst percentages for issue categories *Insufficient Budget* and *Scaling of SOC* are indicated with "—" because questions related to those topics were asked only to our SOC manager participants.

many personal devices will be actively connected to the network at any time:

> *Given the fact that this is a university, the expectation is that each student brings at least four of their own devices to every class. Then you start bringing in the professors and various departments who want their own PCs and researchers who are running high compute performance clusters under their desks. So, there is not a possible way to list all these machines.*

To mitigate the incomplete network visibility issue, avoidable or unavoidable, the participants talked about the solutions that have been working effectively or will potentially work. P*[1], the participant who works for the university with specific requirements on flexible device connections, stated that incomplete visibility had "not been a problem" for them due to effective tracking of all information through their SIEM (Security Information and Event Management), by having authentication clusters, and by actively watching packages. When an incident happens, they look for the person who was authenticated to that machine instead of the machine itself. Also, P4 considered that the visibility problem would be mitigated "if they had a system that would notify them when new machines are introduced on the network."

4.1.2 Inferior Defense Against Specific Types of Attacks

In our interview, we asked our participants about the attacks that they previously encountered from the aspects of *victim specification*, *attacker specification*, and *attack types*. We also asked them about the most challenging attack that they experienced while working at SOCs.

Victim specialty. We categorized attacks as general attacks, industry-specific attacks, and organization-specific attacks, which are attacks targeting the general public, the specific industry sector, and the specific organization, respectively. We asked the interviewees about their experiences on each type of attack. Among all the participants, fifteen participants stated that they mostly encounter the general and basic kind of attacks that are not tailored, especially for an industry or an organization. Ten of our participants stated that they experience industry-specific attacks on occasion, such as tailored phishing attacks exclusively for a particular sector. Eight participants stated that they experience organization-specific attacks in which an attacker targets a specific organization with a clearly defined goal in mind, such as compromising confidential data that is only kept within a particular organization.

Attacker specification. We classified attackers into individual attacks and nation-state sponsored attacks, and we asked the interviewees to compare the difficulty of defending against both attacks. According to nine participants, attacks that are the most difficult to defend against are nation-state sponsored attacks. One of the stated reasons was the nature of these attacks: participants argued that these attackers have bountiful resources, even more than the SOC. Participants also pointed out that these types of attackers have adequate time for the reconnaissance phase and find the best strategy to attack their target network. Regarding nation-state sponsored attacks, P16 said:

> *I think a lot of foreign adversaries are hard. We see traffic coming from another country, another nation and we are able to quickly block that traffic. But, these foreign adversaries, they buy different domain names, different IP spaces. It is very difficult to fully block that particular person ahead of time. So, you are constantly trying to defend against someone that is what I would consider a moving target.*

The participant suggested that a SOC should provide proactive monitoring and a powerful incident response team that has access to high-quality threat intelligence to defend against such attackers.

Attack Types. We divided attacks into remote exploits, phishing, denial of service, and so on, and we asked the interviewees the experience of defending against each type of attack. Phishing is the most common attack mentioned by fifteen participants. Except for

P8, our participant chose not to share further information regarding the attacks that they previously encountered given the confidential nature of those details.

The reason for phishing being the most common attacks mostly varies; however, three participants (P2, P9, and P12) from the same section vector similarly stated that they receive more phishing attempts because their industry sector is more prone to phishing attacks. Specifically, P*[1] gave an example and said:

> *From an airline standpoint, we see that our company is spoofed, and it looked like a web check-in but with malware.*

Furthermore, we asked the interviewees about solutions for phishing attacks. P6 mentioned "using tools that can prevent phishing emails" before they reach their mail server. Two of our participants (P7 and P10), stated that proper training is the "only way" to prevent phishing attacks. Regarding a previous successful phishing attempt, P8 provided details of such an incident that had severe consequences in which the employee was trained specifically for phishing in the last 30 days:

> *A secretary to a researcher was attacked. It was a very well-crafted phishing attack, and the machine got compromised. Based on the information in the mailbox and the system, they were able to pivot and able to hack into the mail server. From there, the attacker was able to monitor the actions that were taken against them and move internally on the network.*

The participant stated that attackers had sent emails on the researcher's behalf to the organization that recognizes the researcher as a trusted source.

Besides phishing attacks, another participant, P13, mentioned Distributed Denial of Service (DDOS) as a difficult and disruptive type of attack, which is used to impact the availability of a service by utilizing multiple hijacked machines, thus hindering legitimate users from using that service [34].

4.1.3 Overloaded and Low-quality Threat Intelligence

Threat Intelligence (TI) is a collection of information regarding security threats [31]. Organizations subscribe to open source and commercial threat intelligence feeds to benefit from such information. Besides, they maintain teams that are dedicated to searching for emerging threats. For SOCs, high-quality TI is paramount in detecting and preventing incidents.

Eleven participants stated that the threat intelligence that they collect from both open-source and commercial feeds is high-quality and useful. However, five participants stated that some feeds provide very large volumes of information, and they are flooded with uncorrelated, industry unrelated, and low-quality data. Regarding the usefulness of their TI, P12 was concerned and said:

> *A lot of our TI is coming from vendors, and our vendors are not the best producing TI. There is not a lot of contextual data in there, which makes them pretty much useless for us. However, sometimes, they prove to be useful, but not every time.*

The interviewer asked P10 if they carefully examine all their threat intelligence feeds, and the participant said:

> *We cannot, it is too much. It was 17 terabytes two months ago, and now it is 20 terabytes. It gets to the point that it is information overload. We are working toward filtering half of the TI that we collect.*

Almost half of our participants (P1, P5, P6, P11, P12, P13, and P15) reported having dedicated TI teams.

4.1.4 Poor Quality Reports and Logs

SOC systems continuously generate reports and logs for many purposes including, but not limited to, informing an analyst of an incident, monitoring the performance of a particular device, monitoring the false positive rate of a tool, or auditing the status of the metric collection. Generating these reports and logs is one of the major and critical daily activity of a SOC.

Twelve participants stated that they are satisfied with their reports and logs; however, five participants had concerns regarding their reports.

P12 was concerned about the lack of context in their reports and said:

> *Reports generated are ambiguous. It is very difficult to add meaning to them. We should add more context to our reports.*

P9 stated that it is difficult to add meaning to the reports and logs and sometimes they do not contain enough context, and therefore are unactionable. The participant said:

> *There may be a lot of data which is also interesting data but maybe not entirely what I need, or it may not give any context to the information which is presented. It takes a lot of time trying to determine how the data fit the alert's context in terms of the infrastructure.*

The most commonly mentioned mitigation by our participants was constant tuning, which is adjusting reports to a better, more optimal state. Three of the participants (P2, P3, and P4), added that tuning is more accurate, faster, and more efficient if the organization develops and uses homegrown tools as this gives them the ability to customize those tools and reports before deployment in the SOC. Moreover, if tuning is necessary after these tools are deployed, the process is faster as the engineers who developed the tools can act on tuning requests faster, as compared to requesting a vendor to make changes. Aside from developing homegrown tools, P4 stated that in their SOC, they have a team dedicated for constant tuning of their reports and logs.

Although P12 mentioned that reports generated by their SOC systems are ambiguous and require improvements, P12's manager thinks that their reporting and logging mechanisms are in perfect condition.

P9 is another analyst participant who disagrees with their manager on this matter. Although their manager thinks that their reports are fine, P9 reported that they are sometimes not actionable. The participant stated that reports do have a lot of interesting information; however, at the same time, they do not have the information that they require for a particular type of incident. As a result, the participant stated that they waste a lot of time researching how the information fits the infrastructure.

4.1.5 High False Positive Rate

When SOC systems classify and indicate a legitimate activity as a malicious one, it is called a false positive.

Fifteen participants stated that false positives are not a major issue for their SOC systems.

Common reasons for having high false positive rates include having low visibility across the board, low SOC maturity, and employee mistakes. Regarding employee mistakes, P11 said:

> *Sometimes, employees do something that they should not in the organization. That is the time when we see false positive ratio go up.*

All the participants manually tune false positives: correcting alerts one by one when they encounter false positives. Regarding tuning, P15 said:

> *We are pretty good at figuring false positives out and fixing them. We call it tuning. We have a pretty good cycle for tuning.*

However, P11 stated that the level of tuning is a trade-off, as too much tuning would cause the systems to miss real incidents. The participant said:

> *False positives are always a balancing act. You can tune out false positives, but you have to be very careful how you do it. If you want, I can eliminate 100% false positives, but I am going to miss some of the true positives.*

4.1.6 Poor Usability of SOC Systems

A SOC can be populated with excellent and top-notch tools and technologies; however; if those tools are extremely difficult to master and use, they will never be fully used. In that case, the SOC analysts would struggle with the tool instead of focusing on the incident.

Nine participants gave high ratings to the usability of their SOC systems and tools. The consensus among them was that usability varies by each tool however, overall, it has not been a major problem.

Participants P2, P12, and P16 reported some concerns.

P2 thinks that if a SOC employee must master many tools at the same time, and if the SOC team is newly formed, the usability level decreases. When the interviewer asked about the level of usability in their SOC, the participant stated that their maturity is increasing over time and usability increases along with it. The participant said:

> *I would put that as a four out of five, it is a very large array of tools that we have and given the maturity. However, the tools that we are using in our daily operations are okay. I would say three out of five a couple of months ago, but now, it is a four.*

P16, who manages an outsourced SOC, stated that, in some cases, clients request that they use a tool that does not have the ideal usability level that they would normally prefer.

P12 argued that usability depends on user education. P12 said:

> *It all depends on user education. If a team has to work on a particular tool, they are fully educated by the team members, and if it is required, the vendor is brought in to train them.*

Regarding usability, we observed from our results that all participant SOCs lack a shared interface that groups all their tools in one location. When the interviewer asked P3 about such an interface, P3 said:

> *That would be a dream come true situation.*

4.1.7 Low Situational Awareness

A high level of Situational Awareness (SA) requires adequate knowledge of the environment and the organization's mission to improve decision-making capabilities [13]. In the context of a SOC, the degree of SA depends on certain criteria, such as the level of employee awareness of the organization's mission, their responsibilities, and their knowledge of the types of attacks and adversaries that the organization may face.

Sixteen participants reported that they have high SA; however, some mentioned that there are still some factors that either make maintaining high SA difficult or decrease SA.

According to P2, the size of their network has an impact on SA. Regarding this, the participant said:

> *The size of the network, interconnections, the overall interactions with other teams. So, it is never going to be 100%.*

Similarly, when the interviewer asked about their level of SA, P8 stated that their SOC monitors many other organizations and added:

> *I would say that we are understanding the majority of the things that we see but due to the fact that there are many organizations that we are monitoring that is an ever amount of change with those organizations.*

Two of our manager participants who manage outsourced SOCs (P5 and P18), stated that they would rate their SA as poor due to not having enough visibility, for the reasons discussed in Section 4.1.1.

4.1.8 Insufficient Analyst Training

In all our participants' SOCs, either internal or commercial training, is provided to employees. Internal training methods include hands-on experiences through simulation platforms, senior employees educating juniors, junior employees shadowing seniors, security lectures, and tool training. Commercial training methods include training programs that are offered by vendors, security certification programs, and tool training packages that are purchased from the vendors along with the related tool.

Two of our participants (P3 and P11), expressed that they do not believe their training programs to be effective. When the interviewer asked P3 about how they would change their current training methods, the participant responded:

> *I would love to change them because the old ones are not working. This is for the majority of the companies; otherwise, phishing campaigns would not be successful; ransomware would not pass through.*

P9, who is a SOC analyst, expressed their disappointment that their organization does not provide any commercial training programs. The participant stated that their organization only provides informal internal training and added that they would prefer formal training that is offered by an external vendor.

P5 stated their concern regarding the importance of tool training and said:

> *One of the biggest issues that I see, most organizations, they buy the new technology, but they do not buy the training. [...] These days tools tend to be extremely complex. [...] Most products are not easy to use and require training.*

4.2 Mismatched Issues

Here, we describe the issues discussed by our participants where they have the least agreement. We selected these issues by observing the gap between the analyst–manager difference in agreement, shown in Figure 2.

4.2.1 Speed of Response and Level of Automation

Three out of five participants who work in an outsourced SOC reported factors that negatively affect their response speed.

P17, who is an analyst in an outsourced SOC, stated that their response speed relies on client's capabilities because, per the provider/-client agreement, they are responsible for only detecting an incident and their client is supposed to respond. When asked about if they could rate their SOC response speed, P17 said:

> *We do not do the final actions to remediate so we cannot be very fast. It depends on the customer's capabilities for the final resolution to be made. Our first response is fast, but depending on the customer overall, it can be slow.*

P16, who manages an outsourced SOC, was concerned about not having enough staff and rated their speed four out of five. P16 said:

> *We are not fully staffed. If we had that staff, I would give it a five.*

P5, who manages an outsourced SOC, stated that visibility is paramount for quick response speed and it tends to be slow because of issues such as potential restrictions in the provider/client agreement or the client's inability to report a full inventory list (Section 4.1.1).

Compared to outsourced SOCs, the ratio of our participants that indicated issues regarding response speed was lower.

We observed that ten out of thirteen participants who work in internal SOCs reported fast response speed without any issues. The other three participants, P2, P11, and P15, also rated their SOC response speed as fast; however, they each provided a reason which affects their response speed negatively.

According to P2, low maturity is the reason for having speed issues. Specifically, when the interviewer asked P2 if they could rate their response speed, the participant responded:

> *I would give a four out of five. Maturity is the reason. Incident response is serious so that they have to coordinate between different departments outside of security. Legal and corporate communications. The house-in procedures are relatively new.*

P15 was concerned about their response speed against new attacks. P15 said:

> *We are pretty good, but there are other things if it is a new type of thing, we are not as good as we should be if it is malware, phishing, like standard attacks we are great but if it is new, we are having problems making sense out of it.*

To improve the speed of response, managers consider automation as an effective and critical approach. P11, who is a manager in an internal SOC, stated that they are not satisfied with the current speed of their SOC and said:

> *No, I am never happy. We are measuring the mean time to mitigate an attack, and we count the priority and severity of the attack, 4 being the least prioritized. In order to mitigate a P0 we have 30 minutes, P1 60 minutes, P2 120 minutes, P3 24 hours, P4 48 hours. Our current success is %87, which is good, but I am not happy.*

The interviewer followed up with a question to inquire about a solution for better speed and asked:

> *What is the solution to increasing that percentage?*

The participant replied:

> *Automation.*

Seven of our manager participants stated that they always want more automation. When the interviewer asked P5 if they need more automation, the participant said:

> *I always need more automation.*

However, P4, an analyst participant, criticized this point of view and said:

> *So, automation is not a Catch-22 type of a problem where it is becoming a buzzword for vendors, and unfortunately, we have a lot of management that sees this more important than the work itself, but not realizing that they are getting less quality.*

Nevertheless, another analyst participant, P7, from another perspective, expressed their satisfaction for automating the metric collection, by stating:

> *Well, every morning, we have to go through all 20 clients and manually get the metrics from them. Before I had to do all of them manually, now they are done in a couple of minutes instead of an hour.*

Lastly, during our interviews, another issue that surfaced was the trustworthiness of automation. When asked if they fully trust their automation, P16 responded:

> *So, we do have regular checks for those systems to make sure that they are working correctly and functioning correctly.*

One of our analyst participants, P6, also argued that automation should not be fully trusted. When asked about the reason, the participant said:

> *Yes, because of false positives.*

4.2.2 Evaluation Metrics

Organizations use metrics to understand if their SOC is performing as intended. Furthermore, these metrics also help to shape plans and identify current problems.

Metrics are of two types: quantitative and qualitative. While quantitative metrics are used for data, such as the number of incidents or the average time of detection, qualitative metrics are used to measure the quality instead of quantity, such as the severity level of an incident.

All of our manager participants stated that they use both qualitative and quantitative metrics, with quantitative being more dominant. Quantitative metrics that our participants mentioned include: number of incidents, number of vulnerabilities discovered, number of tickets per analyst, time of ticket creation, elapsed time of resolution, elapsed time of remediation, elapsed time of mitigation, number of total tickets that are created and resolved, mean detection time, mean response time, mean time of incident closure, time taken to react to an incident, number of incidents that are not closed, and number of known attacks prevented.

Regarding *qualitative* metrics, our participants mentioned only incident severity level and vulnerability severity level.

Although quantitative metrics are dominantly used by our manager participants, some of them consider these metrics inaccurate and ineffective.

When asked about bad practices regarding metrics that are used in SOCs, P14 responded:

> *The metrics that just show you numbers instead of the impact are generally not so effective. Because numbers do not necessarily tell you anything.*

P15 stated that their SOC is only responsible for detection and, after they detect incidents, they hand those cases to other teams and wait for their completion, which renders some metrics inaccurate.

Analysts consider quantitative metrics that are used by their managers ineffective. Furthermore, they consider these metrics as just a tool that their managers use to show false improvement.

When asked if they think that the metrics that are used in their SOC are effective or not, P12 said:

> *Not necessarily, because they do not always show the true effectiveness of a SOC because it is very difficult to measure.*

P4 expressed an extreme disapproval toward quantitative metrics. The participant said:

> *A useless metric can be the number of events because generally, people will not take into account false positive numbers (that are included to the number of events) [...] I think the reason is that the lack of understanding of security of the upper-class management as well as, it is a way to make it seem like your SOC is improving.*

4.2.3 Tool Functionality

A SOC is composed of teams that use those tools to investigate incidents. Some of these tools, such as Security Information and Event Management systems (SIEM), which are typically used as a major tool for managing incidents and consuming logs, are vital for SOC operations. The responsibility for these sets of tools change. Analysts can be responsible for a few sets of tools, whereas their managers are responsible for the whole set of tools in the SOC, including critical tools such as SIEM.

P13, who is a manager, stated that they did not have many cases during the time that they were the manager of the SOC; however, they provided a case in which their SIEM malfunctioned. The participant said:

> *I cannot say we had many but one case we had an issue with a SIEM malfunctioning for a little while, it took a week for the vendor to fix it.*

Another area of the SOC in which managers are responsible is the scaling and integration of new tools. Managers are also responsible for legacy tools and their effects on the SOC. P15, who is the manager, stated their concerns about a legacy tool and said:

> *Every once in a while we are having problems with tools, we are having one right now, we have a legacy tool for a SOC, it is showing its age, we are trying to migrate out of it, but it takes time [...] SOC cannot do its job while it is down, but we have backup systems in place.*

Backup systems act as a fail-safe in SOCs in case of a malfunction. Two of our manager participants, P14 and P18, discussed these mechanisms.

P14 discussed their fail-safe mechanisms in their SOC and said:

> *Yeah, we experienced malfunctions, we have fail-safe mechanisms though we can always roll back and fix things.*

Similarly, P18 stated that they did not have any malfunctioning case before and gave the reason as:

> *We actually got a quite redundant architecture in terms of high availability failover and my experience I haven't seen anything like that.*

SOC managers can also control various teams that belong to or work with the SOC. They can assign teams for such cases and mitigate the problem. Our manager participant, P16, stated that their engineering team takes care of such issues and said:

> *You will have issues with tools all the time and that's where engineers are involved to make sure that these issues are taken care of quickly so we are able to keep those systems up and running, you always have that possibility to have tool issues.*

Unlike their managers, our analyst participants do not think that tool functionality is a problem in their SOC. Three out of eight of our analyst participants indicated not having a tool functionality issue.

P4, who is an analyst in a non-tiered SOC, considers tool functionality issues insignificant for their SOC. The participant stated that manual work should always make up for those functionality problems. P4 said:

> *If there is a situation that a tool-set does not work, we always are to do it manually. If anyone in our group does not have that capability, we train them.*

Maturity is another obstacle regarding tool functionality. If the SOC is young or the SOC team is young, analysts could have issues utilizing the full potential of tools.

P7, our analyst participant who works in a tiered SOC, stated the fact that low maturity could affect them, but did not, and highlighted that their tools do not have any functionality issues. P7 said:

> *We are still young, but the tools that we used worked for us.*

4.3 Other Issues

In our study, we designed manager-specific and analyst-specific questions due to the different scopes of work. Also, the interviewer asked the participants if they have any other problems with their organization's SOC that was not inquired in the prior questions. We grouped their responses in Table 3, and we present other issues that we found as follows.

4.3.1 Lack of a Communication Channel Between Managers and Analysts

Proper communication channels between managers and their analysts are an effective way for analysts to report such cases to their managers. P2, our analyst participant, reported that they have issues regarding their Threat Intelligence (TI) systems; however, their manager disagreed with them stating no issues with their TI systems. As a follow-up, the interviewer asked their opinion on how to eliminate this problem, and the participant stated that they do not have a way to suggest any improvement ideas to their supervisors.

> *If you had the opportunity to talk to your manager about this (TI issue), what would you tell them?*

The participant replied:

> *We can give some feedback on why it would be helpful to use the data. Right now, we may only use the data to kind of look back at and make correlations on versus actually leveraging the data and action. So that would probably be some of the biggest recommendation that we (as analysts) can make is actually using the data, using it to make actions versus using it as a reference point.*

Participant ID	Participant's Response
P1	The constant challenge of defending against ever-changing attacks and adversaries.
P2	Having low SOC maturity.
P3	Need of phasing out from tiered structures. Inadequate training.
P4	Good and skilled people not getting jobs because of not having cybersecurity certifications. Management having a good education but no vision or enthusiasm. Cybersecurity certifications preferred over competence. Following guidelines and blueprints blindly. Utilizing wrong types of metrics.
P5	Analysts' constant need for something new due to the repetition of tasks and tools. Lack of motivation of analysts.
P6	Communication and collaboration problems among teams responsible for protecting the organization's network and assets. Challenge in protecting endpoints, network, and network devices properly, which is sometimes not under SOC's control. Getting everyone to see from SOC's perspective. Need for defense in-depth structure.
P8	Political problems among constituencies and groups of the organization. Challenge in getting trust through the organization.
P9	Not getting the right and necessary data from SOC systems. SOC analysts not focusing on the right direction. Not prioritizing events based on severity. Not leveraging more automation.
P10	Burnout among analysts.
P11	Inconsistent capability and maturity levels among SOC teams and technologies.
P14	Careless efforts and investments to stay cutting edge as a part of the marketing competition. The constant need for catching up with technology. Getting the right tools and training. Having access to the right data. Being unable to generate alerts.
P17	The fact that adversaries will always be one step further. The necessity of adopting an adversarial mindset.
P18	Adopting the wrong ways toward structuring the SOC. Poorly planned investment mistakes.
P7, P12, P13, P15, P16	Stated that every aspect was covered in the interview.

Table 3: Other SOC issues that participants mentioned in their interview.

4.3.2 Insufficient Budget

Six of our manager participants stated that they had sufficient budget for their SOCs; however, some of our manager participants stated their budgetary concerns or constraints.

In some cases, the budget must be approved by organizational powers above the SOC manager. P13 experienced a problem with their superiors. The participant stated that they had a critical plan that they put on hold and said:

> *We have a really good appliance that detects a huge number of incidents in our environment; however, the appliance is not inline, so it does not block the activity. We can see the activity, but we are still allowing it. That is a huge issue, and it is because the budget has not been approved to move it inline.*

Organizations can have several SOCs around the world. In these cases, employees require a travel budget to visit other SOCs and train employees who work in those SOCs. P14 stated that they have a limited budget for training and international travel. P13 stated that they do not have enough funding for employee training and international travels. The participant said:

> *The only budget problem that we have was on training and international travels. That would be the only place that we are not well funded.*

In some situations, organizations make risk-based decisions because they do not have an unlimited budget for their SOC. P14 argued that industry focus also plays a role and said:

> *I think we always want more, but there is a risk-based decision. We cannot spend a billion dollars on cybersecurity. We are not a tool company. We are a financial institution, so we have to balance sometimes.*

Burnout is a prominent issue for SOCs that is also related to lack of budget. One of our manager participants, P10, discussed this by stating:

> *We have happy hours, so everyone goes out to have some drinks, eat dinner outside. Kind of, go interact with your peers, it is really team building thing here and there. [...] I also recommend employees to take some time off when they work six or seven weeks straight. [...] As long as you keep them engaged, they tend to have less burnout, but again it is a financial burden, but we are very lucky because we have the ability to do that.*

4.3.3 Challenge of Scaling SOC Technologies

A SOC is scalable if it allows the integration of new technology or the removal of existing technology without major complications.

All manager participants stated that their SOC is scalable and integrating new technology provides benefits; however, three participants (P5, P14, and P15), added that, in some cases, it was challenging to add new technologies to the SOC.

Regarding these challenges, P14 mentioned the complexity and the difficulty of integrating new technology into their currently active SOC. As an analogy, the participant said:

> *We are flying a plane, and we also need to change the engine while we are flying that plane. So, sometimes, that is the balance we need to maintain.*

5 ACTIONABLE ADVICE AND RESEARCH OPPORTUNITIES

In this paper, we identified mismatched issues, and we see our work as the first step toward resolving these issues. We suggest SOCs, especially managers, follow-up on our findings and communicate with their analysts in terms of automation, evaluation metrics, and tool functionality. For example, for evaluation metrics, we suggest that SOC managers describe the metrics that they use to their employees and justify the reason why they use those metrics. This way, managers will not only receive valuable feedback from their analysts but also ease the feeling of unjustness that their analysts are experiencing. Based on our interview data, we envision three research opportunities regarding SOCs.

5.1 Asset Discovery and Registration

As seen in Table 2, analysts and managers are in agreement that a low level of visibility of devices and network topology is a significant issue. Therefore, a high level of visibility is vital toward SOC success because a SOC cannot prevent an incident that happens in an area that it cannot see.

As one of our participants mentioned in Section 4.1.1, SOCs need a way to discover *every* asset that is active on the network, including *previously-unknown* assets that are newly connected to the network.

To develop such a mechanism is challenging due to many factors such as different industry sectors, the user profile, organizational structure, size of the network, infrastructure, and type of the SOC. The research community should explore such scenarios and suggest ways either to develop novel approaches that would apply to every SOC or be adaptable for each scenario.

5.2 Effective Education

SOC training programs, internal or commercial, are critical to fulfilling the organization's security mission, however our results show that SOC analysts are not satisfied with their training programs.

There have been many research studies that focused on the efficiency and effectiveness of students' learning in virtual environments and yielded promising results [9, 11, 23, 35].

Moreover, there were a few research studies specifically on security education, including a game in the form of an interactive environment, CyberCIEGE, to explore the effectiveness of such environments on learning [26], and another study in which researchers proposed an open-source platform called "i-tee" for simulating security attacks in a virtual sandbox environment [14].

It is also worth mentioning that the United States Army is currently testing a virtual environment for "persistent and realistic training" [1, 7].

The unique environment of a SOC is the perfect candidate for such investigations. The academic community should investigate if *virtual interactive learning environments* can alleviate the current issues regarding employee education, help to improve the efficiency of learning, and fortify the self-efficacy of SOC employees by simulating a real SOC environment.

Furthermore, our participants stated that phishing attacks are still the most prevalent attacks in organizations. These virtual environments might also be useful for increasing security awareness against phishing attacks by interactively simulating their consequences.

5.3 Improved SOC Security Metrics

As Herley et al. [21] stated in their recent work, there has been significant work on properly measuring security, using both quantitative and qualitative metrics; however, "progress here has been slow." Researchers are still trying to create better, more suitable metrics to measure security. However, security metrics that are specific to SOCs are still an open area of research. One specific research direction is to investigate ways to predict the longevity of a vulnerability in different systems of an organization's SOC.

6 LIMITATIONS AND FUTURE WORK

Our study has a number of limitations, and in this section we describe some of those limitations, how the limitations impact the study and results, and the techniques we applied to reduce the impact of those limitations. We also discuss future research directions from this work.

Data Sensitivity. Data that flows through the SOC is sensitive, and the consequences of it being leaked are severe. Given the sensitivity of the topics covered in this research study, it is possible that some participants may not have responded truthfully.

To prevent this from happening, we informed the participants that all questions are optional, and they are free not to answer if they do not feel comfortable answering them before and during the interviews. We believe that most of our responses are accurate, and participants would choose not to answer in the first place if they think they cannot or will not respond truthfully.

Generalization. Another limitation of our research study is that our results may not be generalized to all SOCs, as we had a limited number of interviews. It is worth mentioning that our participants' SOCs are from industry sectors including airline, construction, education, financial services, information technology, and professional services, which covers a wide range of organizations. Furthermore, to improve the applicability and exhaustiveness of our results, we created questions that would cover all aspects of SOCs.

Participant Recruitment. Some of the participants were from large, well-known organizations in which employees have limited time for such research studies. We are worried that some SOC professionals may have declined our request for participation because they wanted to learn the immediate benefit that they will get from this study, which we could not provide at the time. To prevent this issue, we added the following to our recruitment email: *"If this research study is carried out successfully and we receive conclusive results, the limitations of current SOCs will be identified. This outcome may provide potential benefits to the individuals that participate in this study, given that they are part of their organization's SOC".*

We used Snowball Sampling to recruit six of our participants with the goal of recruiting a manager and an analyst from the same organization. In the case that the SOC manager referred to one of their analysts as a participant for the study, the manager chose one of their analysts from a number of analysts. Because of this reason, this selection might have been biased, and also the sample might not represent all of the analysts in that organization. This selection bias and the issue of representativeness does not exist when an analyst referred to their manager as a potential participant since there is only one SOC manager.

Sentiment Analysis. The participants of our study conveyed sentiments through interviews, which can be observed by their tones, actions, and speech. For example, when we asked about the reporting mechanism, one participant responded:

> *Let me explain the setup because it is a little bit complicated (sigh).*

Future research could apply sentiment analysis to the transcripts to understand participants' emotional responses to various topics.

Best Practices vs. Reality Analysis. We found multiple realities that are different from the best practices suggested by the security community. For example, while Zimmerman et al. recommends consolidating computer network defense under one group [55] (Chapter 3), some organizations have "several institutions" to co-work on the response of incident reports, and some organizations even have "two SOCs." Future research could conduct a comparison between the best practices and the reality and investigate whether the best practices are of distinguishable advantage over the other options based on the experience of the interview participants.

Pair Analysis. In our analysis, we discovered contradictory responses from participants who work in the same organization but in different roles as managers and analysts. In this paper, we analyzed matched and mismatched responses of all our analysts and managers because the total number of our participants was not enough to do such a pair analysis. Future research can recruit more participants, and by having more pairs, investigate matches and mismatches among pairs.

Industry Sector Analysis. Different SOC from various industries can have distinct problems. In this paper, we had participants from industry sectors, including airline, construction, education, financial services, information technology, and professional services.

Internal vs. Outsourced SOC Analysis. Different SOC types can have distinct problems. For instance, in our analysis, compared to an internal SOC, we observed that visibility and response speed issues arise more in outsourced SOCs because of the nature of provider/client agreements, a client's limited budget, and a client's inability to cooperate with the provider. Future work can focus on each type of SOCs and analyze their unique issues.

Tiered vs. Non-tiered SOC Analysis. In this study, in total, we had 18 participants; however, only two of them were from a non-tiered SOC. This number was not enough for us to analyze each structure. Given that, in comparison, each SOC hierarchical structure can have superiority over each other in some aspects. Future work can independently study each structure and analyze their unique advantages and disadvantages.

Security Tool Analysis. In this study, we comprehensively analyzed the perspective differences of managers and analysts toward various aspects of SOCs. Among these aspects, we asked our participants what they think about their tools and their functionality issues without going into detail on specific tools and toolsets. Some of the names of the tools that our participants mentioned using are Splunk [48] (SIEM), NitroSecurity products [24] (SIEM), ArcSight [16] (SIEM), McAfee Intrusion Detection System [25] (IDS), FireEye products [15] (Collection of security tools), and Proofpoint [38] (Email Security). Future work can conduct a deeper qualitative and quantitative analysis of specific tools and toolsets that organizations commonly use in their SOCs.

7 RELATED WORK

Past research studies that are related to SOCs focused on improving the efficiency of human analysts. Sundaramurthy et al. [44] adopted an anthropological approach to study SOC environments, and they applied ethnographic methods to close gaps between researchers and participants by studying Computer Security Incident Response Teams (CSIRTs) [46]. As a continuation, they conducted an anthropological study at a corporate SOC for over six months and proposed a model that explains the analyst burnout phenomenon [43]. In their other work, they discussed analyst burnout and reduced effectiveness as adverse effects of failure in conflict resolution [47] and tool-based solutions are proposed to improve SOC efficiency [45].

Axon et al. [2] examined the perspectives of security practitioners by incorporation of non-speech audio into their working environment by analyzing its integration and design requirements. Onwubiko [36] proposed a framework to ensure swift incident resolution and to maintain secure business operations for organizations. The author discussed SOC operations and provided recommendations for best practices related to those operations. Zhong et al. [54] presented a suggestion model that traces the operations of analysts and makes recommendations of actions based on the match with senior analysts' performance. The goals were to avoid novice analysts from being overwhelmed by the influx of incidents and to help them with the triage of those incidents. Goodall et al. [18] presented a visual analytics system, Situ, which they designed for analysts to identify anomalies while watching the network for security events. Janos et al. [27] discussed some good practices such as training for employees, friendly reporting system, and having endpoint detection systems as countermeasures to defend against cybercrimes.

Security incident and event management (SIEM) systems are important because they collect, normalize, and analyze incidents from multiple sources that are handled by security analysts to protect the organization. Therefore, with the increase of more sophisticated and novel attacks, it is important for the SIEM tools to evolve [5]. Additionally, Miloslavskaya et al. [33] shared the concern of having an integrated incident management system for organizations' internal security.

Various research studies focus on the issue of log management because logs are the first piece of information consulted when an attack is encountered. As stored logs are used by organizations for forensics, reviewing, and auditing future incidents, Madani et al. [32] designed a log management functional architecture for network event analysis. Beehive automatically mines and extracts useful data from the overloaded collection of information [52]. Yuan [53] introduced an architecture based on correlation analysis to reduce duplicate alarms, correlate different security events, and suggest measures to tackle security events. In their recent work, Hassan et al. [20] presented a tool, NoDoze, to combat information overload problem that security analysts are experiencing in large enterprises due to the high volume of false alarms.

There are other research studies that we consider related yet did not focus on SOCs specifically. For example, previous work has studied the workplace of IT security professionals [8] and investigated the workflow, decision processes, and cognitive activities in which information assurance analysts engage [10]. Werlinger et al. [49, 51] carried out a participatory observation to identify IT security practitioners' interactions, along with making recommendations on improving tool support for complex security tasks. In another study, Werlinger et al. [50] identified challenges faced by IT security practitioners among human, organizational, and technological factors from semi-structured interviews and analyzed using qualitative description. In a recent study, Stevens et al. [41] presented a case study on the use of formalized threat modeling by security professionals and the benefits it brings to the entire organization's security posture. In other field studies, researchers observed work practices, tools misalignment, and problem-solving strategies of system administrators [3, 19]. Dietrich et al. [12] conducted a qualitative study to understand the perspective of system operators on security configurations and analyze what they perceive as the root cause of security incidents.

In our work, we investigated the potential technical and non-technical issues of SOCs in a more comprehensive manner. Furthermore, we explored manager-based and analyst-based perspectives toward issues and their mitigation by crafting role-specific questions. In our study, we identified several issues that we consider to be critical for SOCs and the overall security posture of organizations.

8 CONCLUSION

In this paper, we conducted a comprehensive qualitative study of SOCs and discovered issues in SOCs. Furthermore, we identified the issues that managers and analysts agree and disagree on, and we proposed advice as well as research opportunities that will improve SOCs.

We believe that our findings will encourage SOC professionals to develop an understanding of each other and put aside their differences. We also believe that this work provides a path forward for future research in this area, bridging the gap between the academic research community and the real-world needs of SOCs.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation (NSF) under Grant No. 1703644. This work is supported by a grant from the Army Research Office (ARO) 92675527, Defense Advanced Research Projects Agency (DARPA) HR001118C0060, Office of Naval Research (ONR) KK1847, by the Institute for Information & Communications Technology Promotion (IITP) grant from KR-MSIT (No. 2017-0-00168), and a grant from the Center for Cybersecurity and Digital Forensics (CDF) at Arizona State University.

REFERENCES

[1] U.S Army. Persistent cyber training environment (pcte). https://www.peostri.army.mil/persistent-cyber-training-environment-pcte. Accessed: 2019-04-16.

[2] Louise Axon, Bushra Alahmadi, Jason RC Nurse, Michael Goldsmith, and Sadie Creese. Sonification in security operations centres: what do security practitioners think? *Internet Society*, 2018.

[3] Rob Barrett, Eser Kandogan, Paul P Maglio, Eben M Haber, Leila A Takayama, and Madhu Prabaker. Field studies of computer system administrators: analysis of system management tools and practices. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, pages 388–395. ACM, 2004.

[4] H Russell Bernard and Harvey Russell Bernard. *Social research methods: Qualitative and quantitative approaches*. Sage, 2012.

[5] Sandeep Bhatt, Pratyusa K Manadhata, and Loai Zomlot. The operational role of security information and event management systems. *IEEE security & Privacy*, pages 35–41, 2014.

[6] Patrick Biernacki and Dan Waldorf. Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163, 1981.

[7] Chris Bing. Here's what the military's 'flight simulator' for cyberwarfare might look like. https://www.cyberscoop.com/cyber-command-training-raytheon-lockheed-martin-pcte, 2018.

[8] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. Towards understanding it security professionals and their tools. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 100–111. ACM, 2007.

[9] Douglas Clark, Brian Nelson, Pratim Sengupta, and Cynthia D'Angelo. Rethinking science learning through digital games and simulations: Genres, examples, and evidence. In *Learning science: Computer games, simulations, and education workshop sponsored by the National Academy of Sciences, Washington, DC*, 2009.

[10] Anita D'Amico, Kirsten Whitley, Daniel Tesone, Brianne O'Brien, and Emilie Roth. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 49, pages 229–233. SAGE Publications Sage CA: Los Angeles, CA, 2005.

[11] Chris Dede, Brian Nelson, Diane Jass Ketelhut, Jody Clarke, and Cassie Bowman. Design-based research strategies for studying situated learning in a multi-user virtual environment. In *Proceedings of the 6th international conference on Learning sciences*, pages 158–165. International Society of the Learning Sciences, 2004.

[12] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1272–1289. ACM, 2018.

[13] Adam Doupé, Manuel Egele, Benjamin Caillat, Gianluca Stringhini, Gorkem Yakin, Ali Zand, Ludovico Cavedon, and Giovanni Vigna. Hit'em where it hurts: a live security exercise on cyber situational awareness. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 51–61. ACM, 2011.

[14] Margus Ernits and Kaido Kikkas. A live virtual simulator for teaching cybersecurity to information technology students. In *International Conference on Learning and Collaboration Technologies*, pages 474–486. Springer, 2016.

[15] Inc. FireEye. Cyber security experts & solution providers. https://www.fireeye.com. Accessed: 2019-08-13.

[16] Micro Focus. Intelligent security operations solutions: It secops software tools. https://www.microfocus.com/en-us/solutions/security-operations. Accessed: 2019-08-13.

[17] Patricia I Fusch and Lawrence R Ness. Are we there yet? data saturation in qualitative research. *The qualitative report*, 20(9):1408–1416, 2015.

[18] John R Goodall, Eric D Ragan, Chad A Steed, Joel W Reed, G David Richardson, Kelly MT Huffer, Robert A Bridges, and Jason A Laska. Situ: Identifying and explaining suspicious behavior in networks. *IEEE Transactions on Visualization and Computer Graphics*, 25(1):204–214, 2019.

[19] Eben M Haber and John Bailey. Design guidelines for system administration tools developed through ethnographic field studies. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology*, page 1. ACM, 2007.

[20] Wajih Ul Hassan, Shengjian Guo, Ding Li, Zhengzhang Chen, Kangkook Jee, Zhichun Li, and Adam Bates. Nodoze: Combatting threat alert fatigue with automated provenance triage. In *Network and Distributed Systems Security Symposium*, 2019.

[21] Cormac Herley and Paul C Van Oorschot. Sok: Science, security and the elusive goal of security as a scientific pursuit. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 99–120. IEEE, 2017.

[22] C. Hill. Security operation center (soc). https://www.nascio.org/portals/0/awards/nominations2018/2018/NASCIO-IL-2018-Cybersecurity-SOC.pdf, 2017.

[23] Gwo-Jen Hwang, Po-Han Wu, and Chi-Chang Chen. An online game approach for improving students' learning performance in web-based problem-solving activities. *Computers & Education*, 59(4):1246–1256, 2012.

[24] McAfee Inc. Device-to-cloud cybersecurity. https://www.mcafee.com/en-us/index.html. Accessed: 2019-08-13.

[25] McAfee Inc. What is an advanced persistent threat (apt)? https://www.mcafee.com/enterprise/en-us/products/network-security-platform.html. Accessed: 2019-08-13.

[26] Cynthia E Irvine, Michael F Thompson, and Ken Allen. Cyberciege: gaming for information assurance. *IEEE Security & Privacy*, 3(3):61–64, 2005.

[27] Fehér Dávid János and Nguyen Huu Phuoc Dai. Security concerns towards security operations centers. In *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, pages 000273–000278. IEEE, 2018.

[28] M. Kan. Boeing's wannacry run-in is a reminder to patch your systems. https://www.pcmag.com/news/360164/boeings-wannacry-run-in-is-a-reminder-to-patch-your-systems, 2018.

[29] Bruce L Berg. *Qualitative research methods for the social sciences*. A Pearson Education Company, 2001.

[30] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *biometrics*, pages 159–174, 1977.

[31] Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhou Li, Luyi Xing, and Raheem Beyah. Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 755–766. ACM, 2016.

[32] Afsaneh Madani, Saed Rezayi, and Hossein Gharaee. Log management comprehensive architecture in security operation center (soc). In *Computational Aspects of Social Networks (CASoN), 2011 International Conference On*, pages 284–289. IEEE, 2011.

[33] Natalia Miloslavskaya. Analysis of siem systems and their usage in security operations and security intelligence centers. In *First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures*, pages 282–288. Springer, 2017.

[34] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[35] Brian C Nelson and Diane Jass Ketelhut. Scientific inquiry in educational multi-user virtual environments. *Educational Psychology Review*, 19(3):265–283, 2007.

[36] Cyril Onwubiko. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, pages 1–10. IEEE, 2015.

[37] Miloslava Plachkinova and Chris Maurer. Teaching case: Security breach at target. *Journal of Information Systems Education*, 29(1):11, 2018.

[38] Inc. Proofpoint. Cyber security solutions from proofpoint. https://www.proofpoint.com/us. Accessed: 2019-08-13.

[39] D. Ritchey. Creating the gsoc: 4 leading examples of successful security operations centers. https://www.securitymagazine.com/articles/87849-creating-the-gsoc-4-leading-examples-of-successful-security-operations-centers, 2017.

[40] Sharma. Why do data breaches happen? https://www.marshall.usc.edu/blog/why-do-data-breaches-happen, 2017.

[41] Rock Stevens, Daniel Votipka, Elissa M Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L Mazurek. The battle for new york: a case study of applied digital threat modeling at the enterprise level. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 621–637, 2018.

[42] Anselm Strauss and Juliet Corbin. Basics of qualitative research: Procedures and techniques for developing grounded theory, 1998.

[43] Sathya Chandran Sundaramurthy, Alexandru G Bardas, Jacob Case, Xinming Ou, Michael Wesch, John McHugh, S Raj Rajagopalan, and Lorrie Faith Cranor. A human capital model for mitigating security analyst burnout. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 347–359, 2015.

[44] Sathya Chandran Sundaramurthy, Jacob Case, Tony Truong, Loai Zomlot, and Marcel Hoffmann. A tale of three security operation centers. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, pages 43–50. ACM, 2014.

[45] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G Bardas, and S Raj Rajagopalan. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Proc. 12th Symp. Usable Privacy and Security*, 2016.

[46] Sathya Chandran Sundaramurthy, John McHugh, Xinming Simon Ou, S Raj Rajagopalan, and Michael Wesch. An anthropological approach to studying csirts. *IEEE Security & Privacy*, 12(5):52–60, 2014.

[47] Sathya Chandran Sundaramurthy, Michael Wesch, Xinming Ou, John McHugh, S Raj Rajagopalan, and Alexandru Bardas. Humans are dynamic. our tools should be too. innovations from the anthropological study of security operations centers. *IEEE Internet Computing*, 2017.

[48] Splunk Technology. Siem, aiops, application management, log management, machine learning, and compliance. https://www.splunk.com/. Accessed: 2019-08-13.

[49] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. Security practitioners in context: their activities and interactions. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, pages 3789–3794. ACM, 2008.

[50] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. An integrated view of human, organizational, and technological challenges of it security management. *Information Management & Computer Security*, 17(1):4–19, 2009.

[51] Rodrigo Werlinger, Kirstie Hawkey, David Botta, and Konstantin Beznosov. Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, 67(7):584–606, 2009.

[52] Ting-Fang Yen, Alina Oprea, Kaan Onarlioglu, Todd Leetham, William Robertson, Ari Juels, and Engin Kirda. Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. In *Proceedings of the 29th Annual Computer Security Applications Conference*, pages 199–208. ACM, 2013.

[53] Shuhong Yuan and Chijia Zou. The security operations center based on correlation analysis. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pages 334–337. IEEE, 2011.

[54] Chen Zhong, Tao Lin, Peng Liu, John Yen, and Kai Chen. A cyber security data triage operation retrieval system. *Computers & Security*, 76:12–31, 2018.

[55] Carson Zimmerman. Ten strategies of a world-class cybersecurity operations center. *MITRE Corporate Communications and Public Affairs. Appendices*, 2014.

APPENDIX

A INTERVIEW QUESTIONS

(1) Do you have separate teams in your SOC?
  (a) How many teams?
  (b) Do these teams work in collaboration?
  (c) Do you have a tiered SOC structure?

(1) How would you rate the visibility of your organization's SOC?
  (a) Do you have a list of all devices/machines on your network?
  (b) What are the reasons for having low visibility?
  (c) What would you need to fix this problem?

(1) Are you mostly experiencing general attacks, industry-specific attacks, or organization-specific attacks?
(2) What types of adversaries are you facing?
(3) Is there any attack/adversary that you find it hard to defend against?

(1) How would you rate your organization's SOC incident response speed?

(1) Are there explicit metrics used to measure the success of your organization's SOC?
  (a) What are these metrics?
  (b) Do you think these metrics are effective?
  (c) How often do you measure your organization's SOC?

(1) Do you have any issues with your organization's SOC budget?
  (a) What is the reason for this issue?
  (b) What was the most critical plan that you needed to forgo because of budget issues?

(1) Is the threat intelligence that you collect high-quality and useful?

(1) Are the reports that you receive from your organization's SOC systems clear and readable?

(1) Are there too many false positives in your organization's SOC systems?

(1) Have you experienced any inconveniences due to tool malfunctions?

(1) Are you satisfied with the current level of automation in your organization's SOC's systems?

Questions for Analysts

(1) Are you permitted to automate parts of your SOC?
(2) Which parts have you automated?
(3) Have you ever felt the need for automation?

Questions for Managers

(1) What kind of automation is needed?

(1) How would you rate the usability of your organization's SOC systems?

(1) Is your organization's SOC scalable?

(1) How would you rate the Situational Awareness (SA) of your organization's SOC?

(1) Does your organization provide training for your employees?

(1) Does your SOC report to one department?
  (a) What is the role of the employee that is in charge of the SOC?

(1) Is your organization's SOC internal or outsourced?

Questions if the SOC is *outsourced*
  (a) Has it always been outsourced?
  (b) What parts of the SOC are outsourced?
  (c) Why did your organization choose to outsource your SOC?

Questions if the SOC is *internal*
  (a) Has it always been internal?
  (b) Why did your organization choose to have an internal SOC?

(1) What is the single most important operation of your SOC?
(2) What does your organization's SOC protect?
  (a) Of these, which is the most critical part that the SOC protects?

(1) How would you rate the maturity of your organization's SOC?

(1) If you had a magic wand, what would be the first problem that you would solve regarding your organization's SOC?

(1) Do you have any other problems with your organization's SOC that was not mentioned in the previous questions?

B MISCELLANEOUS TOPICS AND ISSUES

For completeness, we provide the remaining parts of our interview data.

B.1 SOC Operations and Scope of Protection

Three of our participants, P4, P9, and P12, stated that all SOC operations are tied to each other and have equal criticality. They stated that if any operation fails, other operations would also fail. However, others argued that some operations are more important than others. These include monitoring, incident management, the cycle of prevention, detection and response, and being proactive in which the incidents are aimed to be prevented *before* they happen instead of being reactive in which incidents are mitigated *after* they happen.

Regarding protection, the consensus among participants was that all the entities and parts of the SOC have equal importance when protection is concerned. When the interviewer asked participants to name specific parts, participants mentioned the organization's assets, the corporate network and infrastructure, end-points on the corporate network, and end-users.

However, one of our participants, P12, pointed out that they focus on the most-viable products and high-risk users as a priority.

B.2 Low SOC Maturity

As time pass by, SOCs mature and get stable. Tools that create too many false positives are tuned, employees get experienced, reports get polished, and many more refinements occur. However, this process tends to be very slow, and it takes years for a SOC to have a high level of maturity.

On a scale of 5, 5 being the highest, more than half of our participants rated their SOC's maturity level as 4 and higher. Furthermore, P10 and P11 mentioned that they had a recent maturity assessment in which they scored fairly mature. The rest of our participants who rated their maturity low provided reasons as follows: SOC being established within the last couple of years, having varying maturity levels across the board, recent staff changes, and inefficient communication and collaboration between various teams in the organization. Regarding collaboration and communication, P13 stated that their SOC's maturity is great from the talents perspective but added suggestions to improve maturity level and a relating concern about their current situation. She said:

> *... better integration within the other security teams, better holistic ticketing and reporting because, at the moment, our SOC and people who are actually monitoring and detecting the activities use a separate system than the people who are responding to those activities.*

The participant believes that these suggestions would significantly improve the maturity of the SOC and stated that they are currently working on improving their maturity.

B.3 The Magic Wand that Comes to the Rescue

If provided with a magic wand, participants stated that they would:

- Have more eyes looking for incidents by having more security staff.
- Keep the employees trained.
- Make political issues between groups in their organization go away.
- Create a well-designed ticketing system that would have smooth integration with the currently available tool-sets.
- Assign an unlimited budget to their organization's SOC.
- Put more structure in alert pre-testing before they roll into the SOC.
- Improve their SOC's poor visibility.