Journal of Theoretical and Applied Information Technology
31st December 2020. Vol.98. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A QUALITATIVE STUDY ON SECURITY OPERATIONS CENTERS IN SAUDI ARABIA: CHALLENGES AND RESEARCH DIRECTIONS

SOLTAN ABED ALHARBI [1, 2]

[1]Department of Computer and Network Engineering, University of Jeddah, Jeddah, Saudi Arabia
[2]Department of Electrical and Electronic Engineering, University of Jeddah, Jeddah, Saudi Arabia

E-mail: salharbi@uj.edu.sa

ABSTRACT

The worldwide digital transformation of organizations in all sectors makes them depend increasingly on technology services which indirectly increases the risk of threats and cyber-attacks. Hence, organizations utilize Security Operation Centers (SOCs) to monitor their digital infrastructure for potential cyber incidents. SOC receives and collects information and consequently makes decisions and issues orders or commands. The increment utilization of SOC as a part of cyber security strategy has led to several studies in improving SOC operations. However, few studies have focused on challenges faced by the management and technical staffs working in SOCs. This paper aims to identify these challenges by conducting a qualitative study on SOCs in organizations from different industry sectors in Saudi Arabia. Analyzing the interview data determines the technical and non-technical issues that exist in SOC. The main challenges of SOCs are high false positive rate, low quality of threat intelligence, slow response speed, low visibility on devices and network, and insufficient automation level. Moreover, there are disagreements between managers and SOCs' employee which could affect SOC efficiency and effectiveness if not addressed. The future research directions are presented highlighting the real-world needs of SOCs.

Keywords: *Security Operations Center, Qualitive Study, Data Security, Cyber-attacks, and Security Challenges*

1. INTORDUCTION

The increased dependence on technology changed the hacker's perspective by targeting a large-scale financial profit by implementing more organized cybercrime [1]. This statement is supported by [2] stating that the exploration of malicious activities is increasingly sophisticated, with specific targets and increasingly severe. It also noted that the main aim of the cyber-attacks are businesses, governments, and particular individuals are the existence and dissemination of malware [3]. Some of the current cyberattacks and cybercrime are unprecedented, complex and cause substantive financial losses. For instance, Saudi Arabia's oil conglomerate was attacked in August 2012 by a destructive cyberattack called Shamoon [4]. It is a very destructive wiper malware that wipes out hard drives.

Monitoring business, services and operations continuously and proactively with specialized skills teams is required to cope cybersecurity attacks. Hence, organizations employ a (cyber) Security Operations Center (SOC) that collects and evaluates security related information and consequently handles and protects computer networks from threats and attacks at a central entity in near real-time. Miloslavskaya (2016) has defined SOC as a centralized unit, that handles security issues at an organization level [5], while Zimmerman (2014) has defined it as a team that detects, analyzes, responds, reports and prevents cyber security threats [6]. In other words, the main aim of a SOC is protecting the assets of an organization by detecting and responding to incidents before they get into worst-case scenarios. Although SOCs enhance organizations' security posture [7, 8, 9], the existing SOC serious setup is insufficient where security attacks remain excessive [10].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The failure of SOCs is due to issues related to technical and human-centric. For instance, in 2013, an organization that employs $1.6 million malware detection tool and enforces reasonable security control in place was breached and their date was stolen [11]. Even though the organization was successfully detected and reported the issue to the main SOC, there is no further action was taken by the main SOC. Consequently, the data was breached causing significant losses. Therefore, identifying issues facing SOCs and developing solutions that enhance the effectiveness and efficiency of SOCs are considerably important for security community. Few research works have considered investigating the issues of SOCs, for example, the efficiency of analysts in [12] and the SOCs burnout in [13]. However, there is no comprehensive study on the issues exist in SOCs which make academic community unaware of SOCs issues that must be addressed.

This paper conducts a qualitative study to identify the SOCs issues. The study is based on interviews with security practitioners in SOCs. The study considers Saudi Arabia as a case study because it is one of the most target of cyber conflicts. Several number of SOC employees across different companies were invited to participate, and nine of them from different organizations agreed. The reported issues are analyzed and classified as common and uncommon issues based on degree of agreements. The open challenges in SOCs and research directions to address these challenges are highlighted. The main contributions of this work are as follows: (i) a review of current studies that investigate the challenges and issues that SOCs face, (ii) identifying and analyzing of SOCs in Saudi organizations, and (iii) challenges of SOCs in Saudi's organizations and future research directions.

The rest of the paper is organized as follows; Section 2 presents an overview of SOC, its components, and flow information. Section 3 discusses the related works. The qualitative study on Saudi's SOCs are described in Section 4 including an overview of SOC in Saudi organizations as well as the method of interview and analysis. The results of the interview are analyzed and discussed in Section 5 including the common and uncommon issues. Section 6 presents the future research directions. Finally, the paper is concluded in Section 7.

2. SECURITY OPERATIONS CENTER (SOC)

SOC is a centralized unit that consists of three basic components as shown in Figure 1: analysts, processes, and technology with the aim of protecting an organization from cyber threats [6, 14]. Analysts: the analysts must be skilled and experienced and understand their organization's networks and policies. They examine each alert and obtain if it is an actual attack or not and accordingly decide how the organization responds and initiates the potential response. Process: the organization must define its SOC scope and confirm its authority to accomplish its tasks. In addition, standardized analysis and classification methods must be followed by organization's analysts. This guarantees homogenous investigations of alerts regardless of who is the analyst. Technology: this includes the hardware and the software that utilized in monitoring all assets in a network by generating and processing logs and alerts. Moreover, it filters the flood of data by keeping only the concerned bits and bytes. There are two types of SOCs; (i) Internal SOC: The SOC is managed and operated internally in which it is part of the organization, and (ii)

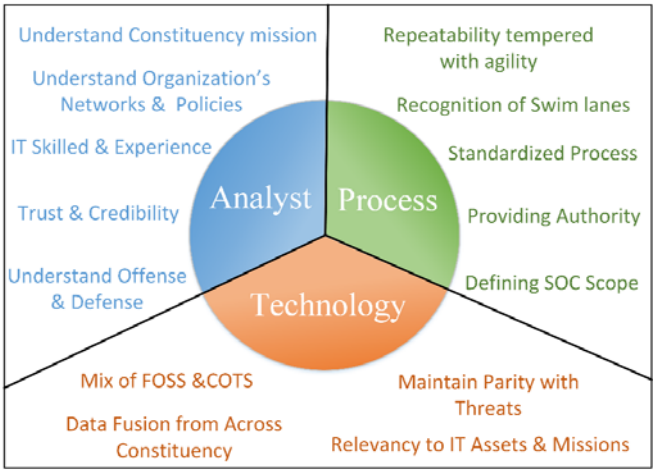

Figure 1: The main components of SOC and its requirements

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

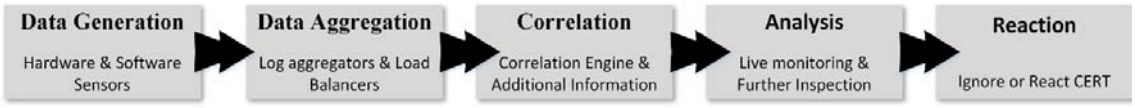

Figure 2: Data Flow in a SOC

Outsource SOC: The organization pays for SOC services to an independent party that manages and operates the SOC.

The data flow in a SOC goes, as shown in Figure 2, through five stages including; generation, aggregating, correlation, analysis and reaction [15].

(i) Generation: Sensors which could be hardware such as routers or software such as antivirus represent the main source of data (i.e., alerts and log data).

(ii) Aggregating: The data generated in the first stage are collected and temporarily stored in this stage. The aggregation process occurs directly on the correlation engine in small setup, while in large setup, it occurs in multiple layers of aggregators for the purpose of load-balancing and arrangement.

(iii) Correlation: This stage represents correlating log data between occurred events and additional sources information. The relevant information about involved hosts, or fetch IP reputation scores might be compiled automatically with the alert. Accordingly, additional second order alerts can be obtained based on the combination. The correlation engine obtains the additional information automatically by filtering events that happened after triggering the alert and linking them to the alert. Moreover, it can obtain automatically domain names, their reputation, and additional records such as configuration files and log files.

(iv) Analysis: The information is analyzed in this stage to determine the responsive action and its necessity. This may require querying further information sources to reach a conclusion which depends on SOC structure and applied analyst tires. For example, querying further information is needed in hierarchical structure where teams who perform live monitoring and teams who investigate events are separated.

(v) Reaction: The responsive actions are conducted in this stage usually by Computer Emergency Response Team (CERT).

SOC operations are complex and require coordination between multiple teams to achieve the tasks. The analysts are considered the brain of a SOC where determining the potential incidents fast and precisely is essential. SOC can be implemented as flat or multi-layer in which the former refers that the analyst who process the alert will conduct the analysis, while a tier-1 analyst in multi-layer forwards suspicious alerts to a dedicated tier for analysis. Large SOC operates 24/7, thus, analysts work in shifts and hands over report about observed and investigated incidents to analyst in the next shift. On the other hand, small SOC operates during business hours and the report is also recorded for analysts to remember where they left off in the previous day [6]. The report could include information about the modification in sensor configurations or the scheduled maintenance of assets. Upon starting their shift, analysts check the report and pull the highest priority alert from the alerts queue or the oldest alert if the alerts are not classified. In addition, each alert contains basic information such as alert timestamp, sensor issued the alert, information of devices involved, what happened before and after the events, and the reasons why is expected to be malicious.

The analysts could classify the alerts as false-positive or irrelevant where there is no further action required, for example, when all assets are known to be immune to a respective vulnerability. However, in many cases, it is not directly clear to distinguish between rogue and benign actions. Upon completing the investigation and reaching to the conclusion, the analyst optionally elaborates his classification to help in getting other analysts respective and improve the SOC. Finally, the analyst informs CERT unit to resolve the issue and get back the organization to the normal state operation.

3. RELATED WORKS

Different aspects of SOC such as setup and operation [6, 14], capability and maturity measurements [16, 17], usability and observations [18, 13] as well as cyber-attack and adversary modeling [19] have been studied in the literature with the goal of improving the efficiency of SOCs. However, the challenges and the difficulties that SOCs face should be identified first to achieve this goal. Hence, several qualitative studies have been presented to investigate the issues faced by SOCs by interviewing practitioners from academic and non-academic operational centers. This section explores these research works and classifies them based on their SOC component scope.

The challenges of SOC process were investigated in [20-23]. The authors in [20] studied

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table I: A Comparison Between Main Related Works

	SOC Component			Interview Participants			Study Sample
	Analyst	Process	Technology	Managers	Analysts	Engineers	
Jaferian, P., et al. 2008.			√		√		Canada
Sillaber, C., et al., 2016		√		√	√	√	Global
Agyepong, E., et al., 2020.	√			√	√		UK
Kokulu, F. B., et al., 2019.	√	√	√	√	√		US
Our Study	√	√	√	√	√	√	KSA

the difficulty of installing and configuring an intrusion detection system, and the significant of the knowledge in SOC operations. In [21], Werlinger et al. conducted a participatory observation on IT security practitioners' interactions and recommended developing a tool to support complex security tasks. The data quality challenges have been investigated in [22] which could affect shared threat intelligence data quality. The study found that the main factors are the integration and consolidation of shared threat intelligence from different sources, and the data's usefulness for an inhomogeneous group of participants. The decision-making process by analysts about risks was studied in [23]. The research findings show that decision making is based on a consolidated effort between analysts, and artefacts that is enabled by communication and awareness. The main challenge of such process is the goal conflict between decision makers specially when context is not considered in specifying security requirements.

Several qualitative studies on the issues and requirement of SOC analysts were presented in [24-26]. A report on incidence response practices of security analysts was presented in [24]. They identified the tasks, skills, strategies and tools that analysts must use to understand security incidents. The authors, in another study [25], identified challenges faced by IT security practitioners among human, organizational, and technological. A framework based on analysts' core functions was proposed in [26] to measure the holistic performance of the analysts. The authors proposed specific key performance indicators (KPIs) including (i) quality of analysts' analysis, (ii) quality of analysts' report, (iii) time-based measures and (iv) the absolute numbers derived from an analyst's tasks.

On the other hand, SOC challenges of utilized technologies and tools were studied in [27-28]. The designing guidelines of security management tools were introduced in [27]. Velasquez et al. [28] reported the challenges of the tools that administrators are used to accomplish various system administration tasks. The cause concept (i.e., signals that cause analysts' action) and norms concept (i.e., adopted IT security standards) are employed to study distributed cognition in SOC environments. A comprehensive qualitative study on the challenges of SOC components was conducted in [29]. Semi-structured interviews were performed with analysts and managers of different SOCs. Several issues related each SOC component was identified. Moreover, the results show that there is usually disagreement level about the main issues of SOC which could affect SOC efficiency and effectiveness.

Table I shows a comparison between the main exist works and our work in terms of investigated SOC component, interview participants and study sample. The main distinction between our work and the others is that we investigated the potential technical and nontechnical issues of SOCs in a more comprehensive manner. The current challenges in SOC were obtained by exploring manager-based and analyst-based perspectives toward issues and their mitigation by crafting role-specific questions.

4. THE QUALITATIVE STUDY ON SOC

The Qualitive research is aligned with our study in investigating the challenges faced by SOCs because the focus of qualitive research is the meanings, concepts definitions, characteristics, metaphors, symbols, and descriptions of things [30]. The methodology of our qualitative study including the study sample and the interview process is presented in this section. Moreover, the significant of SOC in Saudi Arabia and brief description about the known cyberattacks occurred in the past few years are discussed. The research

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table II: Participants in the qualitative study

Participant ID	Position	Organization	Organization Resources
P1	Engineer	Education	Outsource
P2	Engineer	Finance	Internal
P3	Manager	Information Technology	Internal
P4	Engineer	Information Technology	Internal
P5	Manager	Finance	Internal
P6	Manager	Education	Internal
P7	Analysts	Industrial	Internal
P8	Analysts	Education	Outsource
P9	Manager	Industrial	Internal

questions and the analysis of the obtained answers followed the study in [29].

4.1 SOC in Saudi Organizations

The necessity of cybersecurity is linked to overall economic development and the wider utilization of Information and Communication Technologies (ICT). Hence, cybersecurity is considered as a priority in Saudi Arabia because of the continuous economic development and progress towards smart cities. The investors want to make sure that digital services are secure. However, according to a new industry report., 95% of Saudi businesses was hit by cyber-attack in the past year [31]. The report stated that 85% of respondents in Saudi Arabia had dramatic increase in the number of business-impacting cyberattacks over the past two years.

Several cyberattacks to Saudi organizations occurred in the past few years. For example, in August 2012, a destructive cyber-attack called Shamoon has attacked the Saudi national oil company and wiped data from around 30,000 computers [32]. The attack, according to US Secretary of Defense Leon, was originated from Iran with the aim of stopping the flow of Saudi oil [32]. A similar attack in the future could affect financial markets, communication networks, and health and safety services. The cyber-attack cost is high in Saudi Arabia with the average cost of a breach was six million dollars according to 2019 Cost of Data Breach Report [33].

4.2 Interview Method and Analysis

The credibility of the research is achieved by the description of the research process including collection and analyzing of data as well as the obtained conclusions from the research. On the other hand, confirmability is achieved by developing research questions from theory. Thus, the research questions were designed using insight from existing works and are grounded on the roles of SOC's staff. The qualitative research is evaluated by credibility, confirmability and transferability [34]. Moreover, multiple participants from different industries were interviewed to utilize multiple sources of evidence and accordingly achieve the credibility and validity of the study. The interview answers make a deep understanding of technical and non-technical issues that exist in SOC. Nine interviews were conducted with SOC engineers, analysts and managers who work for different industry sectors such as finance,

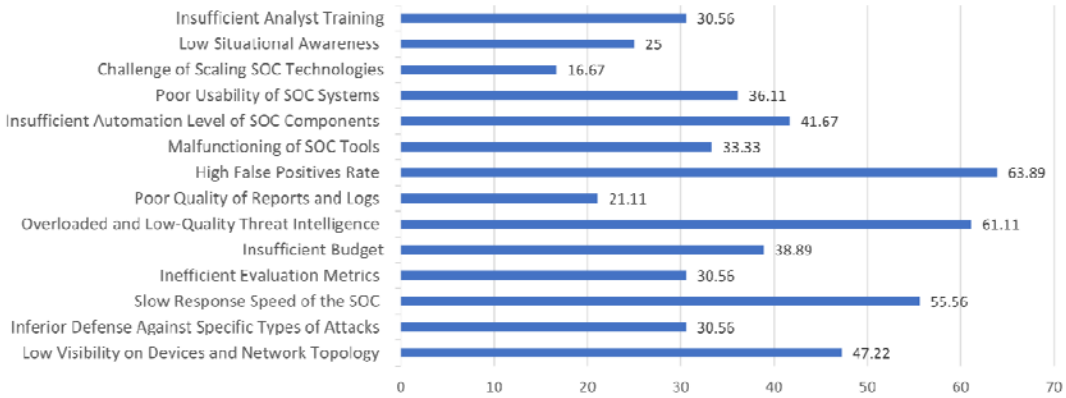

Figure 3: The issues identified by the participants and agreement percentage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table III: Agreement percentage with each issue of SOC managers, analysts and engineers and the mean of the total agreement

Category	Subcategory	Analysts	Managers	Engineer	Mean
Operational Issues	Low Visibility on Devices and Network Topology	50%	25%	66.67%	**47.22**
	Inferior Defense Against Specific Types of Attacks	-	25%	66.67%	30.56
	Slow Response Speed of the SOC	50%	50%	66.67%	**55.56**
	Inefficient Evaluation Metrics	-	25%	66.67%	30.56
	Insufficient Budget	50%	-	66.67%	38.89
Technological Issues	Overloaded and Low-Quality Threat Intelligence	50%	100%	33.33%	**61.11**
	Poor Quality of Reports and Logs	50%	25%	33.33%	21.11
	High False Positives Rate	50%	75%	66.67%	**63.89**
	Malfunctioning of SOC Tools	50%	50%	-	33.33
	Insufficient Automation Level of SOC Components	50%	75%	-	**41.67**
	Poor Usability of SOC Systems	50%	25%	33.33%	36.11
	Challenge of Scaling SOC Technologies	50%	-	-	16.67
Human Knowledge Issues	Low Situational Awareness	50%	25%	-	25
	Insufficient Analyst Training	-	25%	66.67%	30.56

education, industrial and information technology.

Table II shows the participant ID, position, organization and the type of organization resources. In qualitative research, the number of participants is decided according to the following: (i) nature of the study, (ii) practical conditions, and (iii) theoretical saturation. Since the aim of the study is to understand the challenges of SOCs, the high number of participants will make clear interpretations [35]. It was not possible to get more participants in our study due to practical reasons at the studied organizations such as policy and privacy of the organizations, as well as data sensitivity and criticality. In addition, the researcher noticed that most of SOC's staff are not aware of the significant of such study in improving SOCs and coping its challenges. However, the collected answers have given some general patterns with very few contrasting.

5. RESULTS

This section presents SOC issues that are obtained from the survey questions answered by analysts, managers, and engineers. Figure 3 show the issues identified by the participants and agreement percentage between them. Table III shows the percentage of the participants agreed with each issue and the mean of agreement percentage of each issue. We classified the issues based on their mean percentage of agreement between analysts, managers, and engineers into common and uncommon issues. The common issues (bold) have mean percentage more than 40%, while the other issues have less than 40%. The two types of issues are discussed separately in the following sub-sections.

5.1 Common Issues

The common issues with highest agreement rate between analysts, managers, and engineers are discussed in this sub-section including high false positives rate, slow response speed of the SOC, low visibility on devices and network topology, and insufficient automation level of SOC components.

5.1.1 High false positives rate

The false positive refers to classifying a legitimate activity as a malicious. Six participants

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

stated that they experience high false positive rate. The main reasons stated by the participants (P1, P3, P4, P5, P7 and P9) are inefficient evaluation metric, low visibility, and malfunctioning of SOC tools. In addition, the participants (P1 and P9) stated that poor quality of reports and logs may include inaccurate information and consequently mislead them and degrade SOC performance.

5.1.2 Overloaded and low-quality threat intelligence

Threat intelligence refers to the collected information about security threats from open and commercial threat intelligence sources [36]. These information are essential for detecting and preventing emerging threats. Six participants (P1, P3, P5, P6, P8, and P9) believe that the collected threat intelligence does not include high-quality or useful information due to the very large information that are sometime flooded with unrelated, uncorrelated, and low-quality data.

5.1.3 Slow response speed of the SOC

The speed of SOC response to security threats is stated as insufficient by five participants. The threat intelligence is the main reason of SOC slow response especially with new threats and attacks. Since the participants work in outsourced SOC are responsible for detecting threats only, they (P1 and P8) reported that the speed of their SOC depends on client's responding capabilities and quality of reports and logs. On the other hand, the participants work in internal SOC (P3, P4 and P9) stated that the slow response of SOC due to low visibility, low situational awareness, and ineffective evaluation metrics.

5.1.4 Low Visibility on Devices and Network Topology

The low visibility makes SOC staff unable to enforce efficient security operations. Devices and network information, (such as network architecture documentation, full asset inventory, etc.) help in understanding SOC status and responding to threats. Four participants (P1, P3, P4, and P8) reported low SOC visibility. In hierarchical structure SOC, the main reason of low visibility is the lake of communication between IT operations and security teams (P1 and P4) due to improper management or operation by administrators. P1 stated that:

SOC in my organization is under IT department which makes it hard to focus on security issues.

Moreover, P3 reported that the reason of the limited visibility is the lack of experience and knowledge. The low visibility affects the situational awareness and response speed of the participants.

5.1.5 Insufficient automation level of SOC components

Four participants (P3, P5, P6, and P8) stated that their SOC automation level is insufficient which refers to the automatic response to security threats. The participants reported that increasing the level of SOC automation is an effective approach to enhance the SOC response speed. P3 and P6 reported that increasing tier1 monitoring activities is required for SOC system although it must be not fully trusted. P6 said that:

Automating the response and containment are needed with no false positive

5.2 Uncommon Issues

Here, the issues that have least agreements by the participants are discussed where the mean agreement percentage of participant types. The issues are insufficient budget, poor usability of SOC systems, malfunctioning of SOC tools, inferior defense against specific types of attacks, inefficient evaluation metrics, and insufficient analyst training.

5.2.1 Insufficient budget

Three participants (P1, P4, and P8) mentioned that they had insufficient budget for their SOCs. P4 stated the budget issue occurred because the SOC budget is approved by the management above the SOC manager. P4 said:

It is hard to justify needs to top management

In some organizations, SOC budget is included with Information Technology (IT) department. P1 participant said:

No enough financial support for SOC and it is included with IT budgets

5.2.2 Poor usability of SOC systems

The usability of SOC system represents the ability to use and master SOC tools. Setting SOC with excellent and advanced tools and technologies is essential, however, SOC analyst will not be able to fully utilize the tools and detect the incidents. Three participants (P1, P8, and P9) reported poor usability of SOC systems. P1 believes that their new SOC teams are required to master several tools simultaneously, thus, the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

usability is low at the beginning and increases gradually over time.

5.2.3 Malfunctioning of SOC tools

SOC system composes of several tools to investigate security threats in which the managers are responsible of whole set of tools while the analysts are responsible of few sets of tools. The managers are usually responsible also of scaling and integrating new tools. Three participants (P3, P5, and P7) who work as managers in their organization's SOC reported malfunctioning of SOC tools. P3 noticed that tool functionality is affected when the SOC system or teams are new where the tools will not be fully utilized.

5.2.4 Inferior defense against specific types of attacks

The participants were asked about common adversaries faced by their SOC, and if there is any adversary or attack they found it hard to defend against. Most of the participants are facing general and basic attacks that are not designed for specific organization. Among the participants, three (P1, P3, and P4) mentioned that they experienced organization-specific attacks where the attacks have specific target and goal, such as disclosing confidential data. P1 stated that almost all new attacks cannot be defended by their SOC organization due to the lack of training and experience. The employees must be educated about suspicious emails to prevent such attack. P3 and P4 reported that some of Advanced Persistent Threats (APTs) are difficult to defend against by their SOCs.

5.2.5 Inefficient evaluation metrics

Evaluation metrics are utilized in SOCs to understand their performance, help in planning and identifying current problems. Two types of metrics are usually utilized quantitative metrics such as number of threats and average detection time, as well as qualitative metrics such as severity level of attacks. Three participants (P1, P4, and P9) reported inefficient utilized evaluation metrics in their SOCs. P1 stated that there is no specific metrics are used to measure the success of their SOCs and hence they are inaccurate and ineffective. The metrics that the participants are used in their SOCs include Key Performance Indicators (KPIs), red team assessments, audits, time to respond, time to recover, time to back to normal, etc.

5.2.6 Insufficient analyst training

Most of the participants (i.e., 69.44%) reported that their organization provide training courses and workshops. Three participants (P1, P3, and P4) stated that there is no efficient training programs are provided. P3 believes that training will increase the visibility of SOC system and said:

Training, knowledge transfer and more practice/time are essential to increase the visibility of SOC system.

The maturity of SOC organization increases upon providing training programs as stated by P4:

Provide training to SOC teams increases the maturity of SOC organization.

6. RECOMMENDATIONS AND FUTURE RESEARCH DIRECTIONS

There are number of future research directions that can be conducted to enhance the performance of SOC systems. Some of these directions are addressing the limitations of our qualitative study, while others are addressing the research gaps in SOCs that need further investigation. This section discuses these research directions.

6.1 Extensive Investigation on SOCs

This study has the limitation of small sample size which cannot lead to general conclusions. Therefore, a scaling up the study sample is required to conduct a quantitative study and obtain generalized findings. This will help in determining the impact of different factors such as analysts, SOC configuration and other. The study can be extended also to identify the impact of SOC type and the different between their performance including visibility, response speed and their specific issues. Moreover, the impact of SOC structure either flat or multi-layer can be further investigated to obtain the advantages and disadvantages of each type.

6.2 High Quality Threat Intelligence Development

It is difficult to discover errors and inconsistencies in data, thus, utilizing additional data sources will be useful in validating threat intelligence against. It is essential to identify the valuable security data sources that can be integrated to a threat intelligence sharing platform and develop quality assurance algorithms. The significant of the quality of data utilized in threat

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

intelligence platforms and its utilization for security decision making processes in inter and intra-organizational must be emphasized to employee and clients. One of possible future research directions is studying the impact of data quality on the trust of top management and clients in both internal and outsourced SOCs.

6.3 Visibility Improvement

A high level of visibility is necessary for success SOC as most of participants agreed about the important of visibility of devices and networks. SOCs must discover every device on the network including the new connected devise because incidents that occurred in an inviable area cannot be prevented. It is essential to develop efficient discovery mechanisms with the consideration of different factors such as type of industry sector, organization structure, network size and SOC type that can be used with any SOC.

6.4 Education and Training

Education and training are significant for professionals and organizations to ensure maintaining errorless security and preventing sever security events. Educating employees on security information increases the effectiveness of security implementation and awareness. Professional security courses, information security policy announcement, and security awareness posters can be used to ensure good awareness and knowledge. Organizations can also apply penalties on employee that do not follow security instructions. Moreover, workshop about the significant of studies that investigate SOC and its operation to increase the awareness of SOC's staff are required.

6.5 Efficient Evaluation Metrics Development

Employing clear metrics for measuring performance and operation of SOCs could be used as indicators of improvement demand. Developing efficient metrics depends on available data usage and performance criteria selection. Future research is required to obtain good metrics that are suitable of organization sector and SOC effectiveness. In addition, research could be conducted to obtain appropriate operational metrics.

7. CONCLUSION

The risk of threats and cyber-attacks increase dramatically worldwide due to the digital transformation of organizations from all sectors. SOCs are employed to protect organizations and prevent potential cyber incidents. Although several studies with the aim of improving SOC operation have been published, few studies investigated the challenges faced by the management and technical staffs working in SOCs. This paper examined these challenges by conducting a qualitative study on SOCs in organizations from different industry sectors in Saudi Arabia. Different technical and non-technical issues that exist in SOC have been highlighted by the participants in the study. The main challenges of SOCs are high false positive rate, low quality of threat intelligence, slow response speed, low visibility on devices and network, and insufficient automation level. Recommendations and future research directions that highlight the real-world needs of SOCs were presented.

REFRENCES:

[1] Baumard, Philippe. *Cybersecurity in France*. Springer International Publishing, 2017.

[2] CHOO, Kim-Kwang Raymond. The cyber threat landscape: Challenges and future research directions. *Computers & security*, 2011, 30.8: 719-731.

[3] Milošević, N.: History of malware, Digital forensics magazine, Vol. 1(16), 2013, pp. 58-66.

[4] Bronk, C., and Tikk-Ringas, E., The cyber attack on Saudi Aramco. *Survival*, 2013, 55.2: 81-96.

[5] Miloslavskaya, N., Security operations centers for information security incident management. In: *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2016. p. 131-136.

[6] Zimmerman, C., The strategies of a world-class cybersecurity operations center. *The MITRE Corporation, McLean*, 2014.

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

[8] 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-areminder-to-patch-your-systems, 2018.

[9] D. Ritchey. Creating the gsoc: 4 leading examples of successful security operationscenters. https://www.securitymagazine.com/articles/878

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

49-creating-the-gsoc-4-leading-examples-of-successful-security-operations-centers, 2017.

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

[11] Plachkinova, M., and Maurer, C, Security breach at target. *Journal of Information Systems Education*, 2018, 29.1: 11-20.

[12] Axon, L. M., Alahmadi, B., Nurse, J. R., Goldsmith, M., and Creese, S, Sonification in security operations centres: what do security practitioners think?. *arXiv preprint arXiv:1807.06706*, 2018.

[13] Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., and Rajagopalan, S. R., A human capital model for mitigating security analyst burnout. In: *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 2015. p. 347-359.

[14] Shah, A., Ganesan, R., Jajodia, S., and Cam, H., Understanding tradeoffs between throughput, quality, and cost of alert analysis in a csoc. *IEEE Transactions on Information Forensics and Security*, 2018, 14.5: 1155-1170.

[15] Bidou, R., Security operation center concepts & implementation. *avalable at http://www. iv2-technologies. com*, 2005.

[16] Jacobs, P. C., *Towards a framework for building security operation centers*. 2014. PhD Thesis. Rhodes University.

[17] Jacobs, P., Arnab, A., and Irwin, B., Classification of security operation centers. In: *2013 Information Security for South Africa*. IEEE, 2013. p. 1-7.

[18] Mayhew, P., and Alhadreti, O., Are two pairs of eyes better than one? A comparison of concurrent think-aloud and co-participation methods in usability testing. *Journal of Usability Studies*, 2018, 13.4: 177-195.

[19] Bodeau, D., Graubart, R., Heinbockel, W., and Laderman, E., Cyber resiliency engineering aid-the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques. *MTR140499R1, PR*, 2015, 15-1334.

[20] Furnell, S. M., Clarke, N., Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K., Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 2010.

[21] Werlinger, R., Hawkey, K., Botta, D., and Beznosov, K., Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, 2009, 67.7: 584-606.

[22] Sillaber, C., Sauerwein, C., Mussmann, A., and Breu, R., Data quality challenges and future research directions in threat intelligence sharing practice. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. 2016. p. 65-70.

[23] M'manga, A., Faily, S., McAlaney, J., and Williams, C. Folk risk analysis: Factors influencing security analysts' interpretation of risk. 2017.

[24] Furnell, S. M., Clarke, N., Werlinger, R., Hawkey, K., and Beznosov, K., An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 2009.

[25] Werlinger, R., Hawkey, K., and Beznosov, K., Security practitioners in context: their activities and interactions. In: *CHI'08 extended abstracts on Human factors in computing systems*. 2008. p. 3789-3794.

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

[27] Jaferian, P., Botta, D., Raja, F., Hawkey, K., and Beznosov, K., Guidelines for designing IT security management tools. In: *Proceedings of the 2nd ACM Symposium on Computer Human interaction For Management of information Technology*. 2008. p. 1-10.

[28] Velasquez, N. F., and Weisband, S. P. (2008, November). Work practices of system administrators: implications for tool design. In: *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*. 2008. p. 1-10.

[29] Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., and Ahn, G. J. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. p. 1955-1970.

[30] Bruce L Berg. LUNE, Howard; LUNE, Howard. *Qualitative research methods for the social sciences*. Boston, MA: Pearson, 2004.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[31] Tenable, Forrester Thought Leadership Paper: A Custom Study Commissioned, "The Rise Of The Business-Aligned Security Executive", August 2020.

[32] Infosecurity, 'Saudi Aramco Cyber Attacks a "Wake-up Call", Says Former NSA Boss', Infosecurity Magazine, 8 May 2014, https://perma.cc/NXT5-3J57.

[33] IBM Security, The Cost of a Data Breach Report, 2019. https://www.ibm.com/security/data-breach.

[34] Kvale S. Interviews, An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage; 1996.

[35] Albrechtsen, E., A qualitative study of users' view on information security. *Computers & security*, 2007, 26.4: 276-289.

[36] Xiaojing Liao, Kan Yuan, XiaoFengWang, 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.