Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems

Muyowa Mutemwa
Department of Peace, Safety and Security
The Council of Scientic and Industrial Research
Pretoria, South Africa
mmutemwa@csir.co.za

Jabu Mtsweni
Department of Peace, Safety and Security
The Council of Scientic and Industrial Research
Pretoria, South Africa
jmtsweni @csir.co.za

Lukhanyo Zimba
Department of Peace, Safety and Security
The Council of Scientic and Industrial Research
Pretoria, South Africa
lzimba@csir.co.za

***Abstract*—A Cybersecurity Operation Centre (SOC) is a centralized hub for network event monitoring and incident response. SOCs are critical when determining an organization's cybersecurity posture because they can be used to detect, analyze and report on various malicious activities. For most organizations, a SOC is not part of the initial design and implementation of the Information Technology (IT) environment but rather an afterthought. As a result, it is not natively a plug and play component therefore there are integration challenges when a SOC is introduced into an organization. A SOC is an independent hub that needs to be integrated with existing procedures, policies and IT systems of an organization such as the service desk, ticket logging system, reporting, etc. This paper discussed the challenges of integrating a newly developed SOC to an organization's existing IT environment. Firstly, the paper begins by looking at what data sources should be incorporated into the Security Information and Event Management (SIEM) such as which host machines, servers, network end points, software, applications, webservers, etc. for security posture monitoring. That is, which systems need to be monitored first and the order by which the rest of the systems follow. Secondly the paper also describes how to integrate the organization's ticket logging system with the SOC SIEM. That is how the cybersecurity related incidents should be logged by both analysts and non-technical employees of an organization. Also, the priority matrix for incident types and notifications of incidents. Thirdly the paper looks at how to communicate awareness campaigns from the SOC and also how to report on incidents that are found inside the SOC. Lastly the paper looks at how to show value for the large investments that are poured into designing, building and running an SOC.**

Keywords—Cybersecurity Operation Centre, incident response, priority matrix, procedures and policies

I. INTRODUCTION

According to the latest Verizon Data Breach report released during the first quarter of 2018 [1], there were 53 000 incidents and 2 216 confirmed data breaches as cyberattackers hit organisations from small businesses to large enterprises. The loss of customer data could lead to reputation loss or regulatory fines. For an organisation to defend against cybercrimes and cyberattackers, that organisation would need to be able to be aware of potentials threats, detect breaches and events, and respond as quickly as possible to incidents. A Security Operations Centre (SOC) is a centralized monitoring and responding hub consisting of people, process and technologies geared towards creating defences, detecting and responding to incidents. Organization that do not have a SOC and that do not conduct periodical security assessments do not have an understanding of their true cybersecurity posture. That is, they do not know their vulnerabilities neither are they aware when their systems have been breached. In this paper a cybersecurity breach is an unauthorized access to an Information Technology (IT) system.

In this paper a cybersecurity event is when there is a possible hardware or software breach into an IT system. After investigations, an event can either become a false positive, false negative or true negative. False positive is when a security alert was created but there was no malicious activity. False negative is when a security alert was not created but there was malicious activity. True positive is when a security alert was created and there was malicious activity.

In this paper a cybersecurity incident means that there was malicious activity. After investigations, an incident can either be a false negative or true positive. That is there was malicious activity but the alert systems might or might not have picked up the incident.

A. What is a SOC?

As mentioned previous, a SOC is a centralized hub for all network event monitoring and incident response related to cybersecurity events and incidents. SOCs are critical to all organisations when it comes to detecting, investigating and reporting on various malicious activities that occur. According to [2] there are five reasons why an organisation would want to introduce a SOC that is for proactive detection; threat awareness; vulnerability management; awareness of hardware and software assets; and log management.

Proactive detection is having the ability to see when a system's hardware or software has been breached by an unauthorized person. The unauthorized person could be internal (employee) or external.

Threat awareness is having the ability to find vulnerabilities in hardware and software that are used within an organisation. Assigning a score to each vulnerability allows the organisation to know which vulnerabilities are critical and which vulnerabilities should be addressed first. The vulnerability scoring should be assigned using the Common Vulnerability Scoring System (CVSS) scoring mechanisms as found on [3].

Vulnerability management is having the ability to handle the vulnerabilities that are found. There are four ways of managing vulnerabilities that are risks [4] namely risk

978-1-5386-6477-3/18/$31.00 ©2018 IEEE

acceptance, avoidance, limitation and transfer. Risk acceptance is applied in cases where avoidance outweighs the risk itself and in this case an organisation may choose to accept that the particular hardware or software has a risk that can be exploited by attackers. Risk avoidance is applied in cases where an organisation is able to stop using the particular hardware or software that carries the risk. Risk limitation is applied in cases where an organisation can limit its dependency on a particular hardware or software that carries the risk. Risk transfer is applied in cases where the organisation can transfer the consequences of the risk to another organisation.

Awareness of hardware and software assets is having the ability to know which assets are critical and which ones are not so critical. Also knowing the full landscape of the IT environment.

Log management is having the ability to centrally manage all logs from the IT environment and being able to views trends and statistics coming from the logs.

II. SOC TOOLS

In order for a SOC to function, it needs tools. This sections describes some of the type of tools that should be found inside a SOC and what they can be used for.

A. Security Information and Event Management systems

A Security Information and Event Management (SIEM) is a tool that statistically looks at the events from different network sources such as hosts, servers and network endpoints in order to have a common approach to event modelling and security evaluations based on security metrics thereby providing risk analysis procedures [5]. A SIEM tool collects, analyses and reports on log data. A SIEM tool has effective graph generation techniques taking into account known attacks, new attacks, and even zero-day attacks. A SIEM tool will make use of analytical modelling and interactive decision support to provide the relevant security solutions.

B. Threat Intelligence Tools

With a SOC there are different types of tools that can be used to gather threat intelligence. The following are some threat intelligence tools that can be used.

The first is Live News. Live News allows the SOC personnel to view the latest news that has to do with cybersecurity breaches. The latest news might not affect the organisation or its partners to whom the SOC belongs but the information broadcasted can be used as threat intelligence in the event that the victim has a similar business model or similar IT technologies.

The second is Social Media, because hardware and software vendors communicate new vulnerabilities discovered in their products through social media platforms. There are Threat Intelligence platforms that can visualise real-time threat intelligence from social media feeds [6]. A SOC must have access to real time visualization of social media feeds from vendors of their hardware and software products.

The third is a threat Intelligence Platform. A Threat Intelligence Platform is a centralized tool that can pulls feeds from different threat databases based on an organisation's software and hardware assets [7]. This tool must also be able to use the CVSS scoring and Common Vulnerabilities and Exposures (CVE) to classify potential threats.

Lastly, information that is created as output from a SOC. That is data that is generated from the SOC such as vulnerability assessments and reports from investigation or SIEM graphs can be used as threat intelligence to have an idea of vulnerabilities and risks or the type of cyber-attacks that exist in the organisation's IT environment. All tools used in the SOC generate information and that information can be re-used as threat intelligence.

C. Vulnerability Assessment, Investigative & Forensic Tools

The following are types of tools that can be used for investigation and forensics.

Port scanning is a type of tool that can be used to determine the open and closed ports on hosts, servers and network devices. Unused Transmission Control Protocol over Internet Protocol (TCP/IP) ports should be closed. This can be seen a host or server hardening.

Wi-Fi vulnerability assessment is a type of tool that can be used to determine the weaknesses and vulnerabilities that are found in the Wi-Fi network such as testing the encryption algorithm and authentication methods.

Traffic capture and analyser is a type of tool that can be used to capture network traffic.

Sandbox is an IT environment that is similar to the organisation's IT Environment where malware can be executed in isolation without damaging the organisation's actual IT systems. A virtualized network or hypervisor environment can be used as a sandbox tool. Sandboxing allows the SOC to understand what the malware can do if executed in the organisation's IT environment.

Vulnerability Assessment tool is a type of tool that assess websites, operating systems (hosts, servers and network end points) and applications for known vulnerabilities. For applications and operating systems the vulnerability is mainly calculated using the CVSS version 3.0 scoring namely the base, temporal and environmental metrics. For website vulnerabilities the OWASP (Open Web Application Security Project) publishes a report every three years that details the top 10 most widely exploited web application vulnerabilities during that period [8].

Social Engineering assessment tool is a type of tool that can be used to assess the level of cybersecurity awareness within the organisation. There are specific tools that can be used to send emails with attachments or links to employees to test employees' response to suspicious emails.

D. SOC Tool Storage

All SOC tools that are used for investigation or reverse engineering should be store in a central location that can only be access by SOC personnel. A SOC may be mature enough to develop its own tools. These tools should also be stored in the same location. According to [9], the United States' Central Intelligence Agency was hacked and close to 9 000 documents and cybersecurity tools were published on Wikileaks. Therefore it is important that the storage area where SOC tools are kept should be encrypted. And the

machine or virtual machine that houses the tools should be periodically assessed for vulnerabilities. This machine should not be accessible from outside the SOC and preferable it should be on an isolated network.

III. SIEM Data Pulling/Polling Architecture

Technology integration can be direct or indirectly integrated. Direct integration means that technologies can communicate without requiring a third party technology. Indirect integration means that the two technologies will required a third party technology to communicate. Usually newer technologies and technologies nearing their End-of-Life (EoL) can be directly integrated while legacy technologies can only be indirectly integrated.

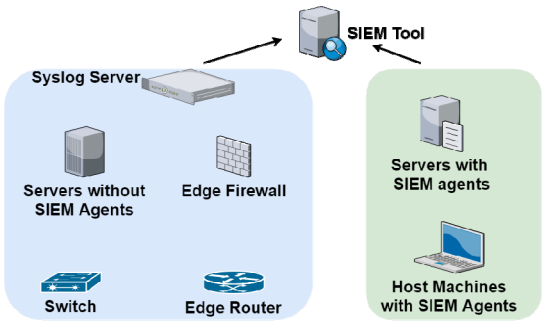

Figure 1: SIEM Agents Polling or Pulling Architecture

Fig.1 shows that in order to pull or poll incidents and events from a server and/or user host machine SIEM agents will have to be installed on the servers and user host machines. Servers that are running legacy applications will more likely have outdate operating systems on which the SIEM agents are not supported. Organisations usually do not have user host machines that are running outdate operating systems, if that is the case the organisation should consider upgrading these host machines or running them in secure virtual containers. All devices that are connected on the network that can install the SIEM agent on them will have send data directly to the SIEM tool.

All other network devices that cannot have the SIEM agent installed will send data to the SIEM indirectly. A network end point can be classified as any device that is on the network that is not a server or user host machine. Such as device could be a Switch, Firewall, Router, Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) and Switch Port Analyser (SPAN). These devices cannot have agents installed on them in most cases, there they will need to forward syslog entries on port 514 to a central syslog server.

1) Syslog Server

On the syslog server the SIEM agent can be installed on it to pull/poll data into the SIEM tool. In the test case presented in this paper, the syslog server had several folders to store and categorize the type of syslog data received. The categories were namely, Firewall, Layer 2 Switch, Router (this includes Layer 3 Switches), Windows Servers, Linux Servers, Other Servers (this could include UNIX) and Network based IPS or IDS.

2) Agent Installation

The SIEM agents on the host machines and servers should be installed as a service on Windows and as a daemon on Linux machines. The Windows service or Linux daemon should be configured to always automatically run on boot-up.

IV. Types of Events to Monitor

Fig. 2 shows all the Windows Event logs. Not all events on a machine should be monitored. Also the events that are monitored on a Windows machine are different to those on a Linux or UNIX machine.

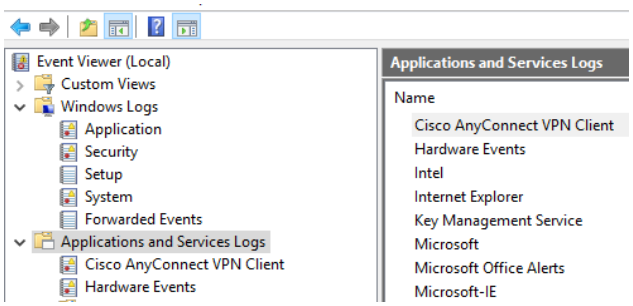

Figure 2: Windows Event Logs

A. Windows Events to Monitor

In this case study the following events were monitored on Windows machines. On the domain controller it is important to monitor the Windows Security logs. On application servers it is important to monitor the Windows Application Logs which gives information on the installation and uninstallation of applications. Applications and Services Logs allows the SIEM tool to capture data from application specific servers such as Domain Name Server (DNS), Document Sharing, Databases, Anti-Virus, etc. can be monitored.

B. Linux Events to Monitor

Fig. 3 shows all the Linux Event logs. On Linux, the operating system and applications store the log files in the /var/log/ location. In order to preserve the integrity of the logs and for security reasons the permission of the /var/log/ folder must be reserved to privilege users. That is only privilege users can write to the folders, subfolders and files. The "syslogd" and "rsyslogd" are the dedicated logging processes. The two main primary logging systems are /var/log/messages and /var/log/syslog.

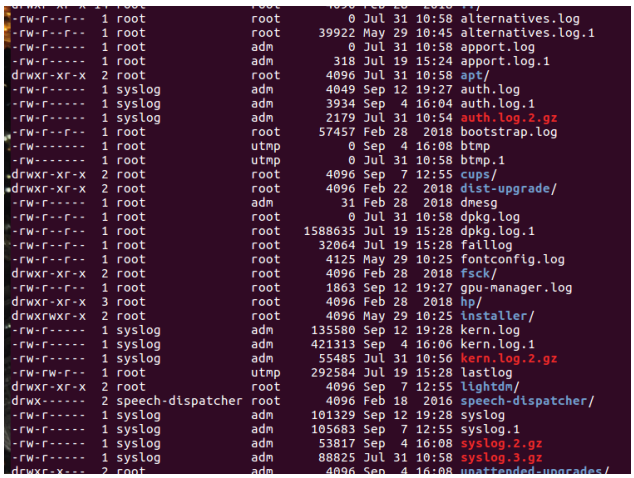

Figure 3: Linux Event Logs

In this case study the following events were monitored and the type of server is also given:

- /var/log/messages: General message and system related logs
- /var/log/auth.log: Authentication logs
- /var/log/kern.log: Kernel logs
- /var/log/cron.log: Crond logs (cron job)
- /var/log/boot.log: System boot logs
- /var/log/secure or /var/log/auth.log: Authentication logs
- /var/log/<application>: Logs for different applications depending on the application name.

C. Network Devices Events to Monitor

At a network level the events that will be monitored depends on the type of the device. Table 1 shows the type of events that were monitored per network device type.

TABLE 1 EVENTS MONITORED FROM A DEVICE TYPE

Device Type	What to Monitor
Firewalls	Session data with its IP 5 – tuples. The 5 tuple being source IP, destination IP, source port, destination port and transport layer protocol. Transaction data that is extracted documents, images, etc should be logged.
Intrusions Detection Systems /Intrusions Prevention Systems	Alert data that is when rules or anomalies are flagged.
Web Filters	Session data with its IP 5 – tuples. Transaction data that is extracted documents, images, etc should be logged.
Email Filters	Session data that is connection events. Statistical data should also be collected.
Endpoint Security (Antivirus & Antimalware)	Extracted data, that is the actual malware that was quarantined.
Virtual Private Network Concentrators	Authentication, authorization and auditing should be logged. Also the session data with its 5 – tuple.
Switches & Internal Routers	Administrative access to the devices, performance logs and type of traffic flowing through should be logged.
Edge Routers	Session data with its IP 5 – tuple.
Domain Name Servers	Transaction data that is queries or responses. Request for external domain names that are known to carry malware.
Authentication, Authorization & Auditing Servers	Alert data that is successful and failed authentication and authorization events. Tracking a successful event at the end of multiple failed events.
Dynamic Host Configuration Protocol Server	Transaction data that is IP assignments.

V. INTEGRATION POINTS

A SOC has people, processes and technologies. These must align with the parent organisation's people, processes and technologies.

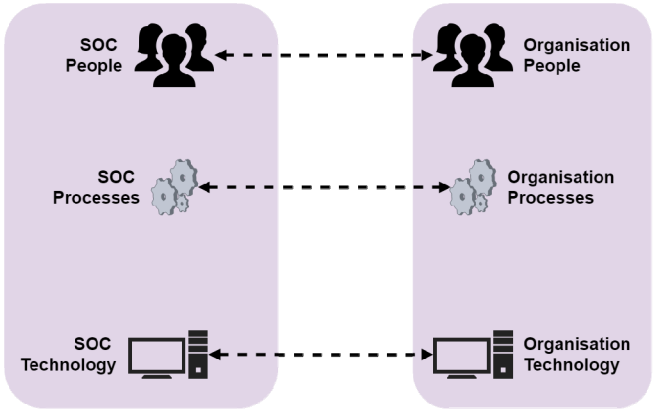

Figure 4: Integration of Poeople, Processes and Technology

A. People Integration

Fig. 4 shows that the people in the SOC must align and work with the people in the organisation. People skills are required to do this. According to [10] graduates engineers need to know that 64 percent of their salaries pays for their communication skills, not their engineering competencies. Communication is one of the key factors when integrating people from different roles in an organisation to work together.

The main challenge here is that cybersecurity is being introduced in an organisation and as a result the key stakeholders of system technologies and processes do not understand their roles with regards to cybersecurity. In the authors' experience the introduction of SOC people into an organisation and the attempt to integrate the SOC personnel and the organisation's key stakeholders was perceived at face value to the key stakeholders as a way in which they will be monitored closely. That is the key stakeholders of system technologies and processes, viewed the SOC personnel as people who will be watching their every move. In developing economies such as South Africa, job security is an important skill set [11]. When a new section is introduced the default view is they are going to take our jobs away and for fulfilment contractors or partners they view the new introduction as the people who will make our contract to be no longer needed. It is therefore important to have kick-off meetings with all the relevant system technologies and process stakeholders in order for them to understand that SOC personal are there to make their security job a lot easier. In particular the SOC manager must be able to clearly communicate the roles and responsibilities of the SOC and its cybersecurity related activities in an understandable language [12]. The SOC manager must be able to make the system technologies stakeholders understand that the SOC is there to ensure the organisation's IT systems, business data, employee data and customer data is secure from cyber criminals. The soft skills of the SOC manager are important for further communication and integration. The system technology owners can guide the SOC to which systems they know houses critical information required to ensure the business continues to function.

B. Technology Integration

A SOC has its own technology. Usually this is the latest versions of software or hardware. On the other hand an organisation has wide range of technology. An organisation's technology can be the latest, approaching EoL or legacy. An

organisation may accept the risk of running legacy technology for reasons such as the cost of acquiring newer technologies does not represent the Return on Investment (RoI), the technology is no longer manufacturer, etc. All these technologies have to be integrated with the SOC technologies.

C. *Process Integration*

A process in a SOC would be the steps that are followed in order to resolve an event. While a process in an organisation would be the steps taken to resolve a help desk call given the call's priority. In order to provide reporting and understand the RoI of a SOC, the SOC processes and the organisation processes have to be integrated. That is SOC processes have to conform to the similar steps as the organisation and as far as possible and be able to use the same systems.

VI. Processes and Procedures Found in an Organisation

A. *Change Advisory Board*

A Change Advisory Board (CAB) is part of the IT Service Management (ITSM) that upholds the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 20000 standard [13]. A CAB is a group of key stakeholders such as subject matter expects and key managerial personnel who are responsible for evaluating changes to the IT environment. Most organisations consider the main role of the CAB to be to authorize the change but it should rather be to provide advice for the change. Another important role of the CAB is to evaluate the risk and mitigation techniques for a particular change together with the potential threat to how a business can be disrupted.

Firstly, by the very definition of the CAB and its responsibility within an organisation, it is important that a member of the SOC be part of CAB. Secondly during implementation and integration of the SOC technologies, it is important that the SOC technologies integration with the organisation's IT environment go through the CAB.

B. *Emergency Change Advisory Board*

An Emergency Change Advisory Board (ECAB) has the same roles as a CAB however this board is a subset of the members from the CAB and is only schedules to address urgent matters so that no unacceptable delays occur [13]. It is important that a member of the SOC team be part of the ECAB as well. Also some SOC security recommendations from investigations may require emergency changes to the IT environment these changes should be processed by the ECAB in order to mitigate potential vulnerabilities or prevent further breaches in an organisation's IT environment.

C. *Incident Management*

Fig. 5 shows that there are 4 methods by which an event can be logged as an incident [14]. Employees of the organisation and cybersecurity expects with the SOC can log calls for the incident to be investigated.

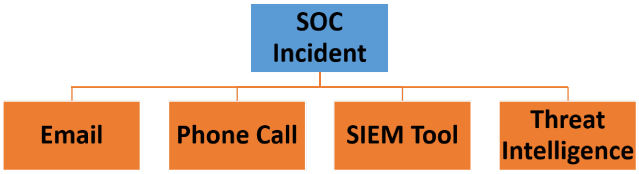

Figure 5: Tools used to Log a Cybersecurity Event

Another integration point between the SOC and the organisation is the introduction of a Cyber Security Team Support. This team is responsible for handling cybersecurity incidents and events logged against the SOC for investigation and resolving [14]. Fig. 6 shows the cybersecurity incident life cycle from detection through to reporting and feedback within the organisation.

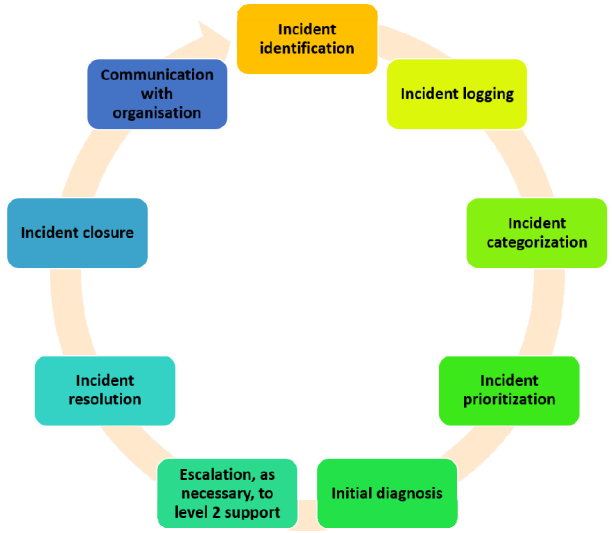

Figure 6: Incident Management Lifecycle

According to [14] there are 6 stages of an incident as shown in Fig. 7.

Figure 7: Six Stages of an Incident

When an incident is first received it is considered new, that is it has not been assigned to the Cyber Security Team Support. Once the incident is assigned it is then in progress in terms of investigation. If there is not enough information or other incidents have a higher priority, an incident can enter the holding or pending stage. An incident will then enter the resolved and finally the closed stage. From the closed state the playbook is updated and recorded in the SOC report.

Every incident should have the correct severity level assigned to it. Table 2 shows the priority matrix for assigning the severity to cybersecurity incidents.

TABLE 2 INCIDENT PRIORITY MATRIX

Incident Severity	Description
Low-priority	No disruption to users or the business and as a work around can be used.
Medium-priority	A few staff or systems are affected.
High-priority	A large number of staff or systems are affected. Potential financial impact on the organisation.

D. SOC Playbook

An important resource in the SOC for incident investigation is a SOC playbook. A playbook contains sub-processes that are step by step guides using distinct systems in order solve an incident [15]. Furthermore a playbook is an unrestrictive collection of previously seen plays (reports and methods) used to detect and respond to security incidents. A playbook is a known error database. The SOC Playbook is a living document which should be updated from time to time.

While investigating a suspicious event the playbook and checklists should prepare the analyst to properly investigate a security event and address the all-important who, what, when, where, why, and how questions that comprise a suspicious investigation.

VII. Reporting on Events and Incidents

Depending on the organisation a SOC report should be provided periodically depending on the need and requirement. The SOC report should provide a very complete view of the statistics of the events and incidents investigated and seen by the personnel in the SOC. The SOC report should also provide the location and identity of critical Windows/Linux host systems. The report should contain Security Incident Investigation Procedures.

VIII. Conclusion

Building a SOC for an organisation is an expensive exercise. However most organisation do not consider the challenges that comes with integrating a SOC into the organisations, in terms of the people, processes and technologies.

As demonstrated in the paper, there are integration challenges that comes with incorporating a SOC into the organisations. As far as possible this paper provided ways in which the challenges can be mitigated or addressed. In order to fully realize the potential of a SOC and allow the SOC to fight against cybersecurity attacks the integration of the SOC's personnel, technologies and processes needs to be correctly integrated with the organisation's personnel, technologies and processes.

In future it would be great to measure the integration levels between the SOC and its organisation. It is not possible to have a 100% integration therefore it is important that the next stage of the research would be to provide information on the minimum level of integration required to allow the SOC to begin functioning to its full ability.

References

[1] Verizon, "2018 Data Breach Investigations Report 11th edition," March 2018. [Online]. Available: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf. [Accessed 13 September 2018].

[2] J. Wilkinson, "5 Reasons You Need A Security Operations Center (SOC)," 15 May 2018. [Online]. Available: https://www.lewan.com/blog/5-reasons-you-need-a-security-operations-center-soc.

[3] FIRST, "Common Vulnerability Scoring System v3.0," June 2015. [Online]. Available: https://www.first.org/cvss/cvss-v30-user_guide_v1.4.pdf.

[4] B. Peterson, "4 Ways to Manage Risk on Web Projects," 13 March 2017. [Online]. Available: https://gracefulresources.com/4-ways-to-manage-risk/. [Accessed 13 September 2018].

[5] C. Andrey and K. Igor, "Attack modeling and security evaluation in SIEM systems," International Transactions on Systems Science and Applications, vol. 8, pp. 129--147, 2012.

[6] J. Mtsweni, N. A. Shozi , K. Matenche, M. Mutemwa, N. Mkhonto and J. J. Jansen van Vuuren, "Development of a semantic-enabled cybersecurity threat intelligence sharing model," in Conference on Information Communication Technology and Society (ICTAS), Boston, 2017.

[7] J. Mtsweni, M. Mutemwa and N. Mkhonto, "Developing a cyber threat intelligence sharing platform for South African organisations," Journal of Information Warfare, vol. 15, no. 3, pp. 56-68, 2016.

[8] A. van der Stock, N. Smithline and T. Gigler, "OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks," 20 October 2017. [Online]. Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[9] S. Khandelwal, "WikiLeaks Exposed CIA's Hacking Tools And Capabilities Details," 7 March 2017. [Online]. Available: https://thehackernews.com/2017/03/wikileaks-cia-hacking-tool.html.

[10] S. Pneena and R. J. Carol, "A message from recent engineering graduates in the workplace: Results of a survey on technical communication skills," Journal of Engineering Education, vol. 90, no. 4, pp. 685--693, 2001.

[11] F. A. Philip, "Job Security in Developing Countries: A Comparative Perspective," Ife Journal of International and Comparative Law, pp. 51-75, 2016.

[12] D. Brecht, "The Skills and Experience Needed to Support A CSIRT, SOC or SIEM Team," InfoSec Resources, 7 February 2018. [Online]. Available: https://resources.infosecinstitute.com/skills-experience-needed-support-csirt-soc-siem-team/#gref. [Accessed 13 September 2018].

[13] S. Watts, "ITIL Change Management & the CAB," BMC, 28 December 2017. [Online]. Available: https://www.bmc.com/blogs/itil-change-advisory-board-cab/. [Accessed 13 September 2018].

[14] BMC, "ITIL® Incident Management," 22 Deccember 2016. [Online]. Available: https://www.bmc.com/guides/itil-incident-management.html.

[15] G. Sanker, "What's an ITIL CAB? A Simple Explanation," itsmtransition, June 2013. [Online]. Available: https://www.ucisa.ac.uk/-/media/files/members/activities/itil/servicetransition/chanage_management/itil_a%20guide%20to%20cab%20meetings%20pdf.ashx?la=en. [Accessed 13 September 2018].

[16] F. Bharathram, "Open Source Playbooks," IncidentResponse, 26 March 2018. [Online]. Available: https://www.incidentresponse.com/open-source-playbooks/. [Accessed 18 September 2018].