A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC)

MSc Internship
Cyber Security

Pradeep Raj Mohanur Jagadeesan
Student ID: X18165672

School of Computing
National College of Ireland

Supervisor: Muhammad Iqbal

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Pradeep Raj Mohanur Jagadeesan

Student ID: X18165672

Programme: MSc in CyberSecurity **Year:** 2019

Module: Internship

Supervisor: Muhammad Iqbal

Submission Due Date: 8th January 2019

Project Title: A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC)

Word Count: 5739 **Page Count:** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC)

Pradeep Raj Mohanur Jagadeesan
x18165672

Abstract

In this 21st century, we have seen a major rise in the use of advanced technological devices. It is well known that these devices generate a huge amount of data. These data end up being the major target for cyber attackers. In order to monitor and protect these devices that are connected to the internet, Security Operation Center (SOC) was developed. The Security operation Center consists of various security professionals. These Analysts constantly monitor the network traffic for any malicious activity in the network. To this date, for operating a Security Operation Center (SOC) there is no standardised framework available. So, this research develops a SOC framework which is expected to improve the performance of the SOC. This research also provides a statistical way to express the performance of the SOC in terms of metrics.

Keyword: *SOC, SIEM, Metrics, framework, MSSP.*

1 Introduction

Security Operation Center (SOC) is considered to be one of the major needs of all organizations that deal with a huge amount of digital data. SOC is a platform that supports detection and responding services to all types of security events. The primary function of the SOC team is to monitor and identify the security threats and neutralize them before it has a major impact on the business functionality of an organization or reduces the impact on the business functionality in case of a successful cyber-attack. SOC services can be externally bought from a Managed Security Service Provider (MSSP)[1] or can set up as an In-House SOC by the organization.

The in-house SOC has various shortcomings. Implementing the in-house SOC requires huge investment in time and money. It also includes conducting additional interviews by Human Resource Team to hire security experts. This type of in-house SOC service is most suitable for large organizations. Whereas the externally bought MSSP service is mostly preferred since it is cost-effective and has their security experts ready to start monitoring immediately. The external service comes in different shape and sizes based on the organization needs which enables them to upgrade or downgrade the service as per their needs. This type of service also has some disadvantages. Here, the analysts need time to understand the network.

[1] https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider

A Security Operation Center depends on Security information and event management (SIEM)[2] tool. SIEM is a software tool that processes the raw logs and checks it along with the rules to find any abnormalities in the network. Figure 1 describes the general architecture of the SIEM tool. The SIEM tool generally has multiple log sources such as firewalls, routers, switches, endpoint security products, IDS, IPS, exchange servers, Active directory server and all network devices. The logs from these devices are sent to the Log collectors of the SIEM and then forwarded to the log processors. Here in the log collectors, the logs are also stored in an external database for backup. The Log processors process the raw logs into readable and understandable logs by parsing the required data from the raw logs based on rules for individual log sources. Then the parsed data is sent to the rule engine where the logs are checked if they match certain conditions. If any match is found, then the desired alert is triggered and shown on to the console by the processor. The rules matched data are stored in an Ariel Search database along with their respective timestamps for future retrieval of the data.

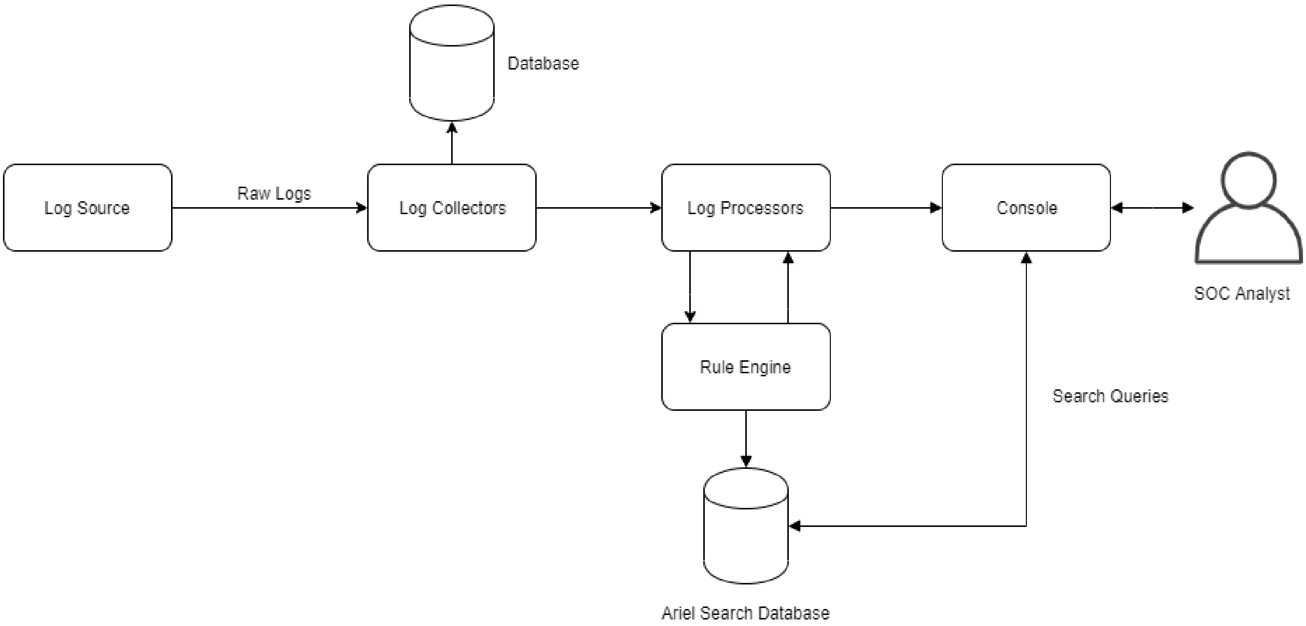

Figure 1 SIEM General Architecture

All these alerts are given a sequence number and are called offences. These Offences are investigated by a SOC analyst. SOC analysts are security personnel who have a deeper understanding of network security and are dedicated to performing IT security operations. These people are trained and know how to act when under cyber-attack. They would monitor the network 24x7. These SOC analysts perform an investigation of the offences and determine what has caused the alerts. If they find it to be malicious then necessary steps are taken to eradicate the risk.

Some of the threats detected by the SIEM are as follows:

- Botnet activity
- Ransomware outbreak.
- Phishing Attack.
- New Vulnerability in the network.
- Suspicious activity.

[2] https://en.wikipedia.org/wiki/Security_information_and_event_management

- Unauthorised Remote Access.
- New Pattern of Activity.
- SQL injections.
- Virus Infections.

Rules are often tuned when false positive offences are detected. The pattern signature is constantly updated from a general commonly shared Trusted Automated eXchange of Indicator Information (TAXII)[3] feed. It is an automated exchange of cyber threat information from all over the world. This gives the advantage of the detection of cyber-attack being executed at an early stage of the attack.

Various logs from a variety of log sources are taken into account when considering an offence. For Example, In case of ransomware attack detection. The ransomware malware would generally start encrypting all the files in the victim machine and try to encrypt all the files in the shared network paths. It would also try to infiltrate into other machines in the same network that the victim is connected to. Here, to identify the ransomware actions in the network, the logs from the windows event logs that contain events of multiple files being deleted will be used. Since the ransomware would encrypt a file and delete the files in bulk. The ransomware would delete shadow copies of windows files. Those logs can be obtained from windows event logs.

Then when the ransomware scans the whole network to infiltrate other machines, those logs can be obtained from network logs of every machine and as well as the endpoint security logs. When the malware encrypts any files in the network, it can be identified using the logs from network logs. Use of endpoint security that detects multiple files deletion across the network is also helpful in this case. Then the firewall logs of the ransomware connecting to the malicious remote Command & Control server IP address can also be used to detect. The vulnerability list of the particular victim machine using the vulnerability management tool. Finally, by correlating all the logs from these various log sources can be used to determine the malicious action by the ransomware and an offence alert is triggered by the SIEM tool. The Analyst once aware of the offence starts to investigate the offence and determines the source of infection and the cause of infection such as vulnerability, missing security patches, etc., and then takes necessary actions such as blocking the IP address of the control server in the firewall and also perform anti-virus scanning on the endpoint machine to eliminate the ransomware.

SOC Services is one of the core important requirement when safeguarding digital data. Especially when highly sensitive data is in place. SOC services are currently trending in areas of Financial, medical and government Sectors. Since these sectors are currently being targeted the most. Although there are many MSSP providers in the market, there are not many providers that show how efficient their SOC service is since there is no known way to estimate the efficiency or the performance of SOC in terms of metrics. It is also noted that there is no Standardised Framework for Managing a Security Operation Center (SOC) unlike other frameworks such as ITIL, COBIT, NIST etc., that are specialized for managing IT services and Information Security. Hence, this paves a way for the requirement of a framework that also provides a guideline to weigh the performance in terms of metrics.

[3] https://taxiiproject.github.io/about/

2 Related Work

2.1 Framework Based on the managerial part:

In this section literature review is provided from various IEEE research papers. One of the papers authored by Stef Schinag (2015) states a framework for SOC. In the paper, the author has explained about the various implementation forms of the SOC. Five areas of the SOC activities such as intelligence function, a baseline security function, Monitoring function, pentest function and forensic function have been covered in that research. The author has also included the management part of the SOC such as employing a new analyst and managing the SOC when senior highly skilled analysts leave the job. In the paper, the author recommends not to create a number of SOC since there were a limited number of very skilled analysts. It can be clearly seen from the paper that the research was performed more based on purely managerial part and not the technical part of SOC.

2.2 Machine Learning Model:

In the research paper authored by Charles Feng (2017), the author states a framework for a security operation Center using user-centric machine learning. The author focuses on eliminating the false positiveness in the SOC using a machine learning algorithm. The author plans to achieve the net results based on two groups of people. One group are the data scientists who have every skill to create a machine learning algorithm but has no idea of information security. Whereas the other group consists of skilled SOC analyst who has deep knowledge of information security and wants to develop a machine learning algorithm.

The author aims to perform machine learning based on every individual user. So that it makes it simple to eliminate the false positive and analyse the alerts. In this research, the author uses the raw data from Symantec security logs and the logs from DHCP, IDS/IPS, FTP and web server for analysis. Users were assigned a label to perform the machine learning model. Here initially the text mining[4] was performed on the previous analyst's investigation notes. Keywords such as "Risky" was marked for users after text mining. This was used to perform the machine learning model and identify risky users. This research solely aims to remove false positiveness and does not convey about the other technical or managerial part in setting up or running a SOC.

2.3 SOC Implementation on Cloud:

In the paper by Tala Tafazzoli (2016). The author provides a methodology to implement and setup SOC in a cloud environment. Usually, the implementation of SOC in a cloud environment is difficult and has a lot of challenges, specifically in a multitenant cloud

[4] https://en.wikipedia.org/wiki/Text_mining

architecture Since the performance of the SOC on a multitenant cloud can be drastically decreased by noisy neighbour tenant on the cloud platform. This research paper by the author aims to receive and analyse logs from the OpenStack[5] cloud environment. The author explains how SOC is connected to the OpenStack platform in order to protect and prevent attacks in the cloud environment. The author has used Zabbix[6] agent on the cloud platform to connect to the SOC. Zabbix agent is an opensource monitoring tool that can monitor and collect the logs from virtual machines, servers, cloud services and send it to a remote location. Here the listening port of the SOC is made open to the internet and the agent is configured to send the logs to the SOC. The author explains only about the implementation in the cloud and doesn't explain about managing the SOC or improving the efficiency.

2.4 Weighing scheme:

The research paper written by Pierre Jacobs (2013) proposes the classification of security operation Center. The author also provides a method to weigh the SOC capability which can help the SOC managers to determine the status and identify the growth of the SOC. This can help MSSP providers to market the SOC using these growth scores. Here in this research, the author has combined the number of existing security management frameworks such as ISO 27001[7] and SANS critical security control[8] frameworks. The author has defined six maturity model for SOC in order to assign a weight to SOC. The author has used NIST security maturity levels to be integrated with SOC. This paper doesn't take much consideration of the technical aspects of SOC.

Natalia Miloslavskaya (2016) has defined research on security operation center based on existing ones. The author has explained the main functions and key indicators of incidents. The author brief about the incidents in IOT resources in terms of tracking and recovery. Jung-Shian Li (2010) proposes a mobile agent-based Security operation center. The drawback of a generic SOC is that it is in a fixed location which makes it vulnerable to a single point of attack. If that SOC location fails there is no means of backup SOC. Hence a mobile SOC might be useful.

Alexander Tolstoy (2016) propose a taxonomy for processing big data in the security operation centres. An IS policy and IS incident management policy was used in the research. Attacks are classified based on the nature of the threat and the IS incidents were classified based on the destructive actions of the threat. Alexander Tolstoy states that the taxonomy is suitable for use in any organization and is ready for developing the threat and intruder model. The threat model might include vulnerabilities exploited, possible loss, potential damages. An intruder model can also be defined to formally classify intruders based on motivations.

[5] https://wiki.openstack.org/wiki/Main_Page

[6] https://en.wikipedia.org/wiki/Zabbix

[7] https://www.iso.org/isoiec-27001-information-security.html

[8] https://www.sans.org/critical-security-controls/

3 Research Methodology

This Section proposes the methodology that is used in this research. This research is to develop a framework that provides a guideline to improve the efficiency of the SOC. Also, it provides a point-based system to estimate the efficiency of the SOC in terms of metrics. The research is performed based on 3 aspects as given in Figure 2 SOC triangle:

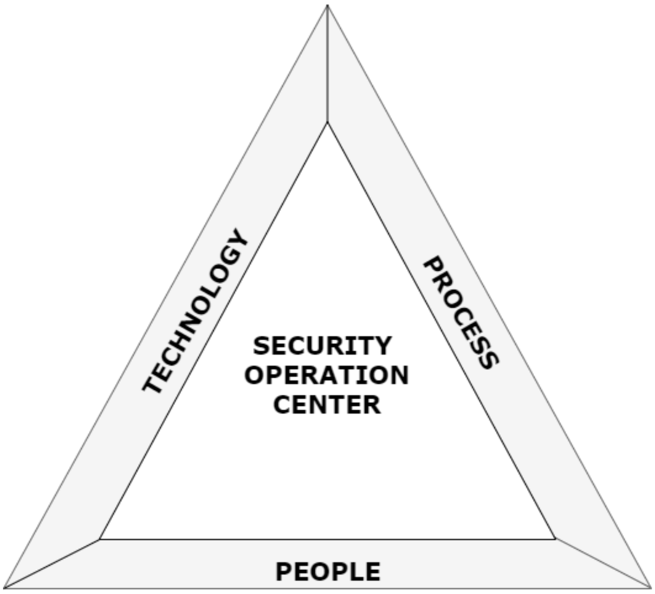

Figure 2 SOC Triangle

The technology aspects consist of various key technical guidelines to set up a security operation Center such as hardware requirements, processing power, software requirements, Log source requirements etc., Whereas the process defines the type of process such as handling an incident, training staff, Workflow, Periodically keeping the analysts updated with new technologies, Encouraging the analysts to take up Certification, Reporting, Analysing the performance in metrics etc., The people aspect consist of the type of people employed at the SOC.

4 Design Specification

This section describes in brief about the three aspects of the security operation Center key triangle used in this research.

4.1 People:

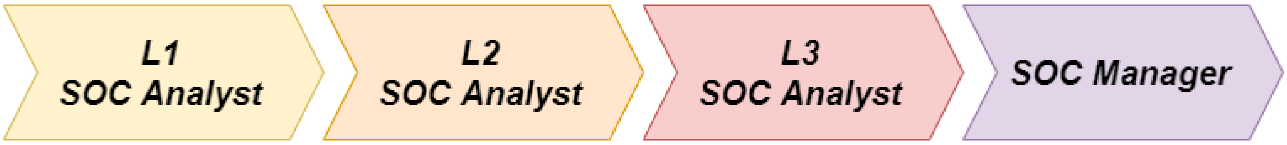

Figure 3 SOC People Types

In a security operation Center, there must be a minimum of 3 analysts namely Level 1, Level 2 and Level 3 SOC Analyst along with one SOC manager. Every individual analyst has their own responsibilities and capabilities. They are dedicatedly assigned to perform a certain task. The L1 SOC analyst is responsible for reviewing the latest offences or alerts to determine the urgency and also determine false positive ones. The L1 analysts are also responsible for creating a ticket and also forward the details of the offence to next level L2 analysts in case the offence requires deeper analysis. The analyst would perform vulnerability scans and configure monitoring tools. The L2 SOC analyst is responsible for identifying the affected system and collect asset data such as source and destination IP address, the process running in the system etc., for further investigation. This analyst would determine and suggest recommendation to overcome or eradicate the threat. This analyst takes a role in the recovery process at the time of successful cyber-attack. The L3 SOC analyst has the responsibility to perform threat hunting and identify advanced stealth threats. The analyst would also provide recommendations to optimize the security monitoring tools based on the threat hunting discoveries. The analyst would also review asset data and vulnerability assessment data while performing threat hunting. Next, the SOC manager is a highly skilled person who looks after the health and growth of the SOC team. The SOC manager supervises the SOC team and manages escalation process and reviews reports. The SOC manager measures the SOC performance and acts as a medium between the non-technical management people and the technical SOC analyst. The SOC manager also helps the analyst when need. The SOC manager plays a major role in managing the SOC by encouraging and guiding the analyst towards a greater goal.

4.2 Technology:

In terms of technology used in SOC, SIEM tool is the heart of the Security Operation Center. There are two types of SIEM tools available in the market. One is opensource SIEM tool such as AlienVault OSSIM, Apache Metron etc., and other is Commercial tools such as IBM Qradar, Splunk, Micro Focus ArcSight ESM, LogRhythm etc., IBM Qradar stands unique in the market with various features. Use of commercial SIEM tools is preferred over opensource tools since the commercial tools have various features and support from the developer. Not many opensource tools were found to have frequent updates and support. Commercially available tools are more reliable when compared to opensource tools. In order to have the tools running, powerful computation power and machine is required. High-end machines give hand in improving the efficiency of the SOC performance. Since all the siem tool alerts and offences are based on real-time traffic and log analysis. A poor computation power leads to slow processing of the raw logs leading to delayed alerting or sometimes may lead to failure of alerts which in turn successful and unnoticed cyber-attack. A powerful CPU with processor core of over 48 cores is recommended. The RAM used in the machines should be over 64GB for machines handling a larger amount of logs processing. Disk throughput is also important in data processing since the speed of disk assess should high for quick data retrieval. The disk throughput can be calculated using:

Throughput = [IOPS] * [Block Size]

Where IOPS stands for Input Output Operations per second, and the block size defines the block size of the log file written to the storage. The use of Solid-State Drive (SSD) increases the IOPS but this hardware is expensive compare to general Hard Disk Drives (HDD). In this case, HDD with higher transfer rate can be used. Disk Space of over 6TB is recommended for the use with medium-sized SOC. When it comes to database storage, the use of an external storage database is recommended. The use of the database that is default embedded with the siem tool does not support storage and extraction of a large amount of data. The embedded database appears to uncomfortable when searching for particular logs. PostgreSQL database use is suitable in this case. Since the network monitoring takes place in realtime, use of Gigabit Ethernet (IEEE 802.3ab) or faster fibre optics network is best suitable.

In SIEM log collector and log processor are used. The log collector collects the raw logs and stores it to a database and the log processor converts the raw logs into understandable format and process it. They both perform a major role in SOC. Use of more number of collector and processors based on the size of the SOC is recommended. When multiple collectors are set up close to the log source the data collection and processing occurs in parallel and reduces the time delay. 6 collectors and 6 processors are required for a medium-sized SOC in order to obtain maximum performance. Setting up of in-house SOC is recommended since it offers controlled architecture and no need of the data being accessed by third-party SOC providers.

Log sources are network devices which generate network logs that are sent to the siem tool. The analyst would normally correlate the logs from multiple network device and determine if an event is a threat or not. If logs are available from very fewer network devices then it would be difficult to determine the nature of an event. Configuring the SIEM to receive logs from many log sources such as IDS, IPS, DNS server, DHCP, windows logs, server logs, file access logs, endpoint security, firewall logs, WAF logs, web server logs, Honeypot, user activity logs, database logs etc., would enable easy understanding of the event and it would also increase the accuracy of the threat detection by the analyst. In SOC, the use of a good ticketing tool is required in order to create tickets and keep track of the threat being handled. This also provides easy communication and understanding by the non-technical management people and network team who supports during threat blocking.

4.3 Process:

In a Security Operation Center, the SOC analyst performs the monitoring and analysis of the network event using SIEM tool. When a network event matches with the rule that is categorised as a malicious action, then an alert action is triggered called “Offence”. It is also given a unique Offence id. This offence list is available in the SIEM console. The analysts start the investigation using the offence id. The below flowchart illustrates the workflow in SOC.

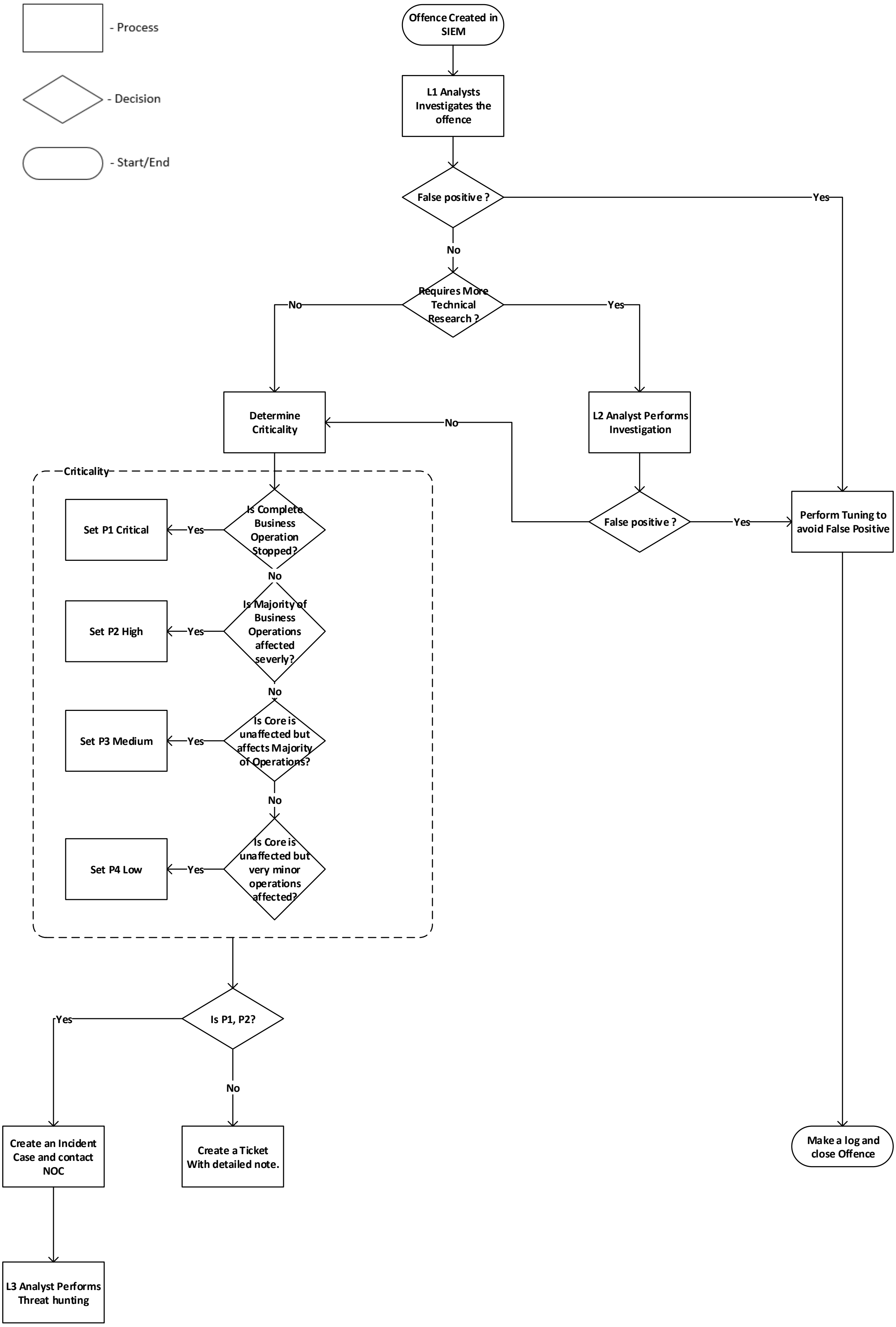
- Process
- Decision
- Start/End
Offence Created in SIEM
L1 Analysts Investigates the offence
False positive ?
Yes
No
Requires More Technical Research ?
No
Yes
Determine Criticality
L2 Analyst Performs Investigation
No
False positive ?
Yes
Perform Tuning to avoid False Positive
Criticality
Is Complete Business Operation Stopped?
Yes
Set P1 Critical
No
Is Majority of Business Operations affected severly?
Yes
Set P2 High
No
Is Core is unaffected but affects Majority of Operations?
Yes
Set P3 Medium
No
Is Core is unaffected but very minor operations affected?
Yes
Set P4 Low
Is P1, P2?
Yes
No
Create an Incident Case and contact NOC
Create a Ticket With detailed note.
Make a log and close Offence
L3 Analyst Performs Threat hunting

Figure 4 SOC Flow chart

Algorithm:

```
Step 1: START
Step 2: Offence created in SIEM tool.
Step 3: L1 Analyst starts investigation.
Step 4: IF False positive THEN
Step 5:                 Perform Rules tuning
Step 6:                 Make a log and close offence STOP.
Step 7: ELSE IF Requires More technical research THEN
Step 8:         L2 Analyst Performs Investigation
Step 9:         IF False Positive THEN
Step 10:                GOTO STEP 5
Step 11:        ELSE GOTO STEP 12
Step 12:        ELSE Determine Criticality
Step 13:                IF Complete Business Operation Stopped THEN
Step 14:                SET Criticality as P1 Critical
Step 15:        ELSE IF Majority of Business Operation affected Severely THEN
Step 16:                SET Criticality as P2 High
Step 17:        ELSE IF Core is unaffected but affects Majority of Operations THEN
Step 18:                SET Criticality as P3 Medium.
Step 19:        ELSE IF Core is unaffected but very minor operations Affected THEN
Step 20:                SET Criticality as P4 Low.
Step 21: IF Criticality P1 OR P2 THEN
Step 22:        Create Incident AND Contact NOC
Step 23:        L3 Analyst Performs Threat Hunting
Step 24: ELSE Create Ticket with note.
Step 25: STOP
```

One step among the workflow is the offence investigation. This step is important since an analyst uses full potential and knowledge gained through experience to determine the real nature of an offence generated. The whole Investigation process goes as shown in figure 5.

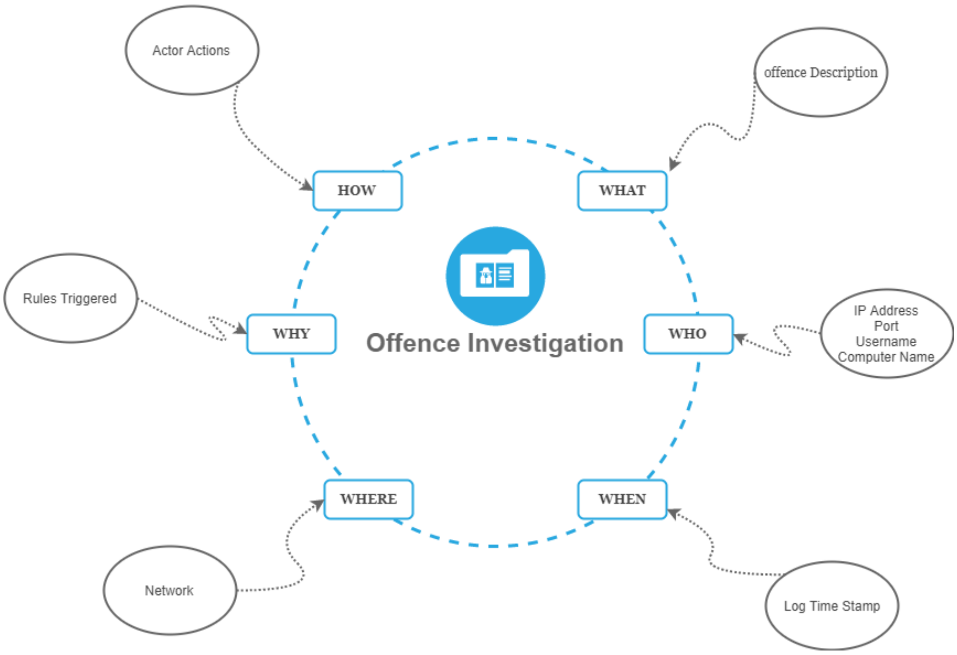

Figure 5 Offence Investigation

The investigation phase consists of these 6 Questionaries which needs to be answered,

1. What is the nature of the event?
2. Who caused the event?
3. When did the event occur?
4. Where did the event occur?
5. Why did the event occur?
6. How did the event occur?

What?

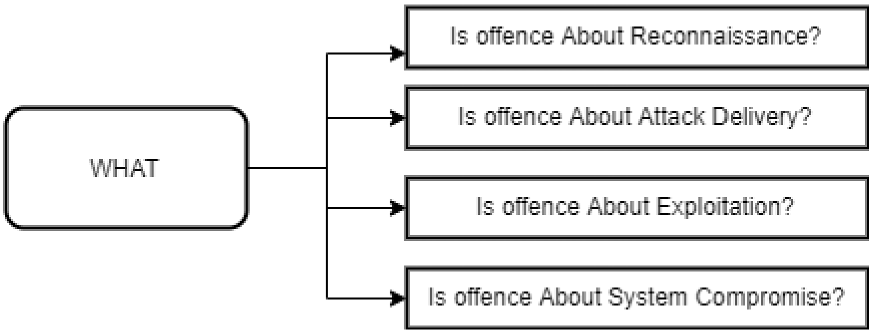
WHAT
Is offence About Reconnaissance?
Is offence About Attack Delivery?
Is offence About Exploitation?
Is offence About System Compromise?

Figure 6 What?

The description of the offence about the event gives the analyst an idea of what type of threat the analyst is going to investigate. For example, if the offence descriptions describe a remote port scanning attack. Then the analyst decides to look for a remote IP address. It is the initial step of the offence investigation.

Who?

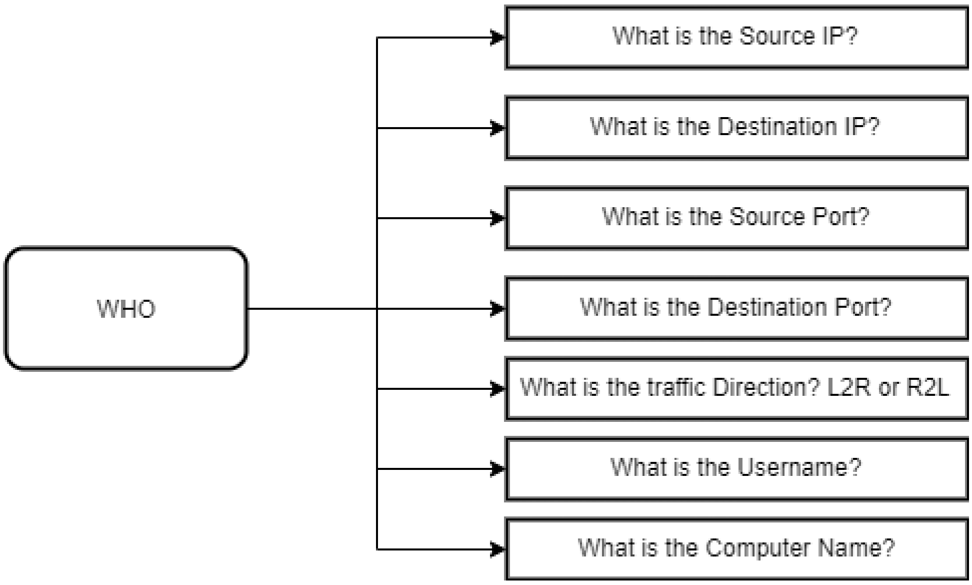
WHO
What is the Source IP?
What is the Destination IP?
What is the Source Port?
What is the Destination Port?
What is the traffic Direction? L2R or R2L
What is the Username?
What is the Computer Name?

Figure 7 Who?

The analyst next has to determine who is the event related to. This can be answered by determining the IP address of the user, username, computer name and also if the traffic direction is from remote to local or from Local to the remote destination. This clearly gives an idea of who is the relevant user.

When?

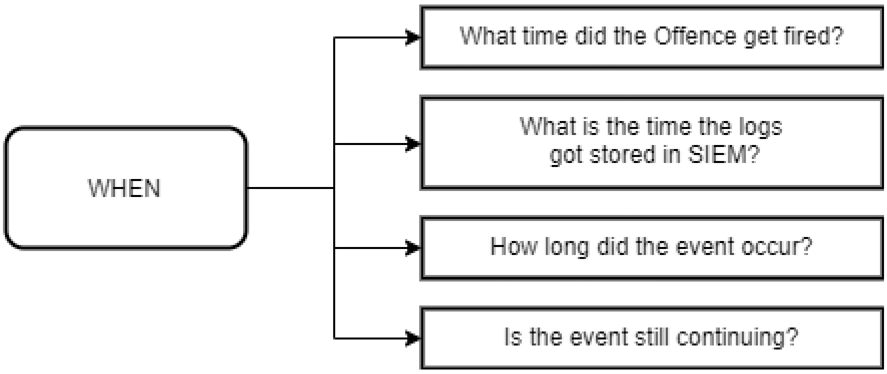
WHEN
What time did the Offence get fired?
What is the time the logs got stored in SIEM?
How long did the event occur?
Is the event still continuing?

Figure 8 When?

The analyst now has to determine the exact time of the event from the event logs so that the time can be correlated with other events belonging to the same user. The analyst would need to know when the alert has triggered the offence and exact time of when the logs got stored in the SIEM database, exact time length the event occurred for. This gives the analyst to get an idea of the time frame to set as the scope of analysis.

Where?

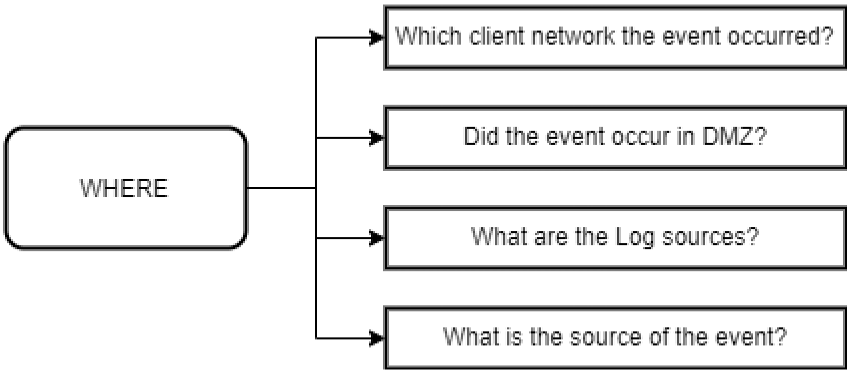
WHERE
Which client network the event occurred?
Did the event occur in DMZ?
What are the Log sources?
What is the source of the event?

Figure 9 Where?

The analyst in this stage has to determine the exaction network location of the event. The analyst would check which client network the event occurred (in case of multi-tenant[9] SOC) and check if it is a DMZ network. Then the type of log source of the event such as firewall, endpoint security, IDS etc., will be estimated. This gives the analysts a view of how the attack would have occurred.

Why?

In this step, the analyst has to determine which rule is asSOCiated with the offence in order to determine if the rule was a valid one. Then the analyst must also ensure if any rule was updated recently. Since the alert might have been caused by a misconfigured rule that was changed recently.

[9] https://whatis.techtarget.com/definition/multi-tenancy

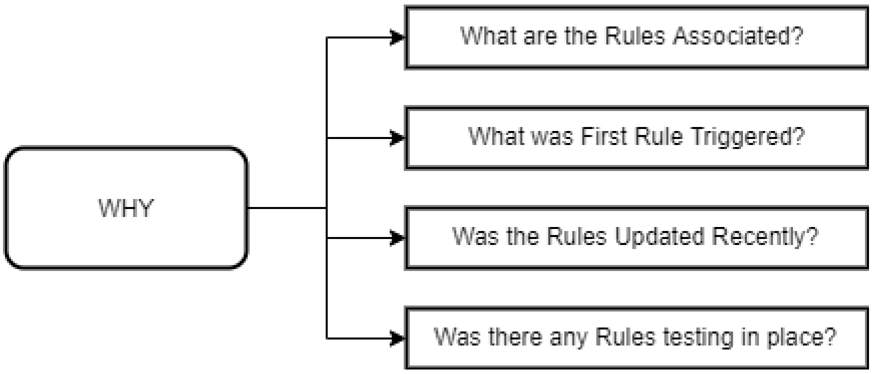
WHY
What are the Rules Associated?
What was First Rule Triggered?
Was the Rules Updated Recently?
Was there any Rules testing in place?

Figure 10 Why?

How?

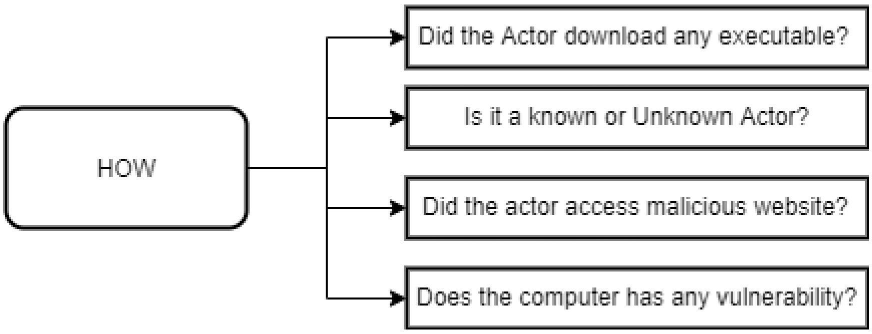
HOW
Did the Actor download any executable?
Is it a known or Unknown Actor?
Did the actor access malicious website?
Does the computer has any vulnerability?

Figure 11 How?

In this phase, the analyst has to determine how did the event happen by checking the event logs. The analysts will have to know what the user was actually doing during the time of the event. It must be also checked if the user was downloading any executable which might have been malicious or if the user had accessed any malicious website or if the user had opened any malicious attachment from spam folder in the mailbox. This helps in understanding the offence.

Having all the questionnaires answered the analyst would have come to an end of the investigation and would be sure about the nature of the event. If the analysts find it be malicious then the analyst would proceed to the next stage to determine the criticality of the offence in terms of P1(Priority 1) being critical, P2 High, P3 Medium and P4 Low. Then as per the workflow steps would be continued.

The recommended time frame for an analyst to investigate an offence and come to a solution is 15 Mins per Offence. Adhering to strict timeframe would enable the analyst to take up the next offence. This would also improve the performance of the security operation center since the time taken to complete investigating all the offence will be lowered.

Another aspect that must be included is, the regular training of the employee to learn something new. The SOC manager must ensure that regular knowledge-sharing activity must be conducted in the workplace so that this enables the analyst to gain more knowledge about

SOC. The SOC manager must also encourage all the analysts to take up certifications in the field. This makes sure that the analysts are certified and prove to have the skills. This also adds an advantage to marketing purpose. More the analyst gets skilled more the performance of the SOC.

5 Implementation

The Proposed framework and guideline can be used as a base to create points-based metrics table as shown in table 1 below:

Model	Requirement	Smaller SOC Score	Medium SOC Score	Larger SOC Score
Processors Core	Less Than 4 Core	2	1	0
	4 cores	3	2	0
	16 cores	5	3	1
	24 cores	5	5	3
	48 cores	5	5	5
RAM Memory	Less than 16GB	1	0	0
	16GB	3	1	0
	32GB	5	3	1
	64GB	5	5	2
	128GB	5	5	5
Disk Throughput	Less Than 500MB/s	1	0	0
	500MB/s	3	1	0
	1000MB/s	5	4	2
	2000MB/s	5	5	5
Hard Disk Storage	Less than 6TB	2	1	0
	6TB	3	2	0
	12TB	5	4	2
	40TB	5	5	5
Network - Gigabit Ethernet Usage	Yes	5	5	5
	No	2	1	0
Database	Embedded Database	3	1	0
	External Database	5	5	5
Log collectors Used	Less than 2 Nos	1	0	0
	2 Nos	2	1	0
	6 Nos	5	3	2
	8 Nos	5	5	5
Log Processors Used	Less than 2 Nos	1	0	0
	2 Nos	2	1	0
	6 Nos	5	3	2
	8 Nos	5	5	5
Log Source Minimum Count	Less than 4	1	1	0
	4	2	2	1
	6	3	3	2

	8	5	5	5
Use Of Ticketing Tool	Yes	5	5	5
	No	2	1	0
Configured TAXII Feed	Yes	5	5	5
	No	2	1	0
Skilled Analyst Count	Less than 3 Nos	2	1	0
	3 Nos	5	2	0
	6 Nos	5	3	2
	8 Nos	5	5	5
Average Time Taken to Complete One Offence	15 Mins	5	5	5
	20 Mins	5	3	2
	25 Mins	3	2	1
	Greater than 25 Mins	1	1	0
Regular Employee Training In place	Yes	5	5	5
	No	3	2	0
Certified Soc Analyst	Yes	5	5	5
	No	2	1	0

Table 1 SOC Metrics Table

The point-based metric system for measuring the performance of SOC has been classified into 3 types of SOC Business levels based on the average amount of logs received per second by the SIEM tool. This is shown in table 2:

Threshold Avg Logs Per Second	SOC Size
80,000	Large
40,000	Medium
20,000	Small

Table 2 SOC Size classification

The points are calculated to a total of 5 points for each model depending upon the SOC size. Then finally the average is calculated and converted in percentage to give the performance score of SOC in metrics. The calculation is shown as :

Performance Score = (Avg(Models Score points)/5)*100

6 Evaluation

In this section, the metrics scoring system will be evaluated across sample data since currently there is no access to real data to be used for this research due to data privacy.

6.1 Experiment 1

In this evaluation, we will consider a Medium level SOC that has an average input of 48000 Logs per second. The table shows the sample requirement input of a Medium Level SOC company.

Model	Requirement Input	Points of 5
Processors Core	4 cores	2
RAM Memory	32GB	3
Disk Throughput	500MB/s	1
Hard Disk Storage	Less than 6TB	1
Network - Gigabit Ethernet Usage	No	1
Database	External Database	5
Log collectors Used	2 Nos	1
Log Processors Used	2 Nos	1
Log Source Minimum Count	4	2
Use Of Ticketing Tool	No	1
Configured TAXII Feed	Yes	5
Skilled Analyst Count	Less than 3 Nos	1
Average Time Taken to Complete One Offence	25 Mins	2
Regular Employee Training In place	No	2
Certified Soc Analyst	No	1
	TOTAL	**29**

Table 3 Evaluation 1 Table

From the above table we can calculate the performance score as follows:

Performance Score = (Avg(29)/5)*100
= ((1.93333)/5)*100
= (0.386666667)*100
Performance Score = 38.66

From the above calculation, we can see that the performance of this Medium level SOC is around 39%. The performance percentage seems to be low since in this evaluation, a company that doesn’t follow the framework is chosen and the relevant sample data was used.

6.2 Experiment 2

In this let us assume the same Medium Level SOC company that adheres to the Framework guideline and recommendation to be used in this evaluation.

Model	Requirement	Medium SOC
Processors Core	24 cores	5
RAM Memory	64GB	5
Disk Throughput	1000MB/s	4
Hard Disk Storage	12TB	4
Network - Gigabit Ethernet Usage	Yes	5
Database	External Database	5
Log collectors Used	6 Nos	3
Log Processors Used	6 Nos	3
Log Source Minimum Count	8	5
Use Of Ticketing Tool	Yes	5
Configured TAXII Feed	Yes	5
Skilled Analyst Count	6 Nos	3
Average Time Taken to Complete One Offence	15 Mins	5
Regular Employee Training In place	Yes	5
Certified Soc Analyst	Yes	5
	TOTAL	**67**

Table 4 Evaluation 2 Table

From this table the performance score is calculated as follows:

Performance Score = (Avg(67)/5)*100
= ((4.466666667)/5)*100
= (0.893333333)*100
Performance Score = 89.33

The performance score of this evaluation is 89% which is a good score for this medium-sized soc.

6.3 Discussion

In both evaluation performed it can be clearly noted that performance score varies drastically when guidelines are followed. This can be used to rate any SOC business and compare it even while purchasing External SOC services.

7 Conclusion and Future Work

In this research, a framework was defined based on true experience during the internship term. The framework can be useful for setting up a new SOC. However, migration to this framework from an existing SOC might be time-consuming as more changes have to be performed which might interrupt the current production setup. In this framework, the individual need of the clients was not considered in the case of Multitenant SOC. The other issue in using the framework is the cost of setting up of the SOC would expensive since the key requirements in this framework are set high. But, having borne the cost this might increase the performance and the quality of the SOC team. The performance metrics evaluation has also added an addon to this framework through which performance can be constantly checked. In Future, the cost disadvantage can be minimized by analysing and developing guideline based on the individual client's requirement while keeping the quality of the SOC in a steady state.

References

Schinagl, S. (2015). A Framework for Designing a Security Operations Centre (SOC) - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7070084 [Accessed 18 Dec. 2019].

Feng, C. (2017). A user-centric machine learning framework for cyber security operations center - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/8004902 [Accessed 26 Dec. 2019].

Tafazzoli, T. (2016). Security operation center implementation on OpenStack - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/7881927 [Accessed 27 Dec. 2019].

Jacobs, P (2013). Classification of Security Operation Centers - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/6641054 [Accessed 27 Dec. 2019].

Miloslavskaya, N. (2016). Security Operations Centers for Information Security Incident Management - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/7575854 [Accessed 28 Dec. 2019].

Li, J. (2010). Implementation of the distributed hierarchical security operation center using mobile agent group - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/5533775 [Accessed 28 Dec. 2019].

Tolstoy, A. (2016). Taxonomy for Unsecure Big Data Processing in Security Operations Centers - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/7592716 [Accessed 28 Dec. 2019].

Ncsc.gov.uk. (2016). Security operations centre (SOC) buyers guide. [online] Available at: https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide [Accessed 28 Dec. 2019].

Hu X. (2006). Security Operation Center Design Based on D-S Evidence Theory - IEEE Conference Publication. [online] Available at: https://ieeexplore.ieee.org/document/4026457 [Accessed 1 Jan. 2020].

Sans.org. (2019). Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. [online] Available at: https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf [Accessed 1 Jan. 2020].

Owasp.org. (2017). OWASP Security Operations Center (SOC) Framework Project - OWASP. [online] Available at: https://www.owasp.org/index.php/OWASP_Security_Operations_Center_(SOC)_Framework_Project?veaction=edit [Accessed 1 Jan. 2020].

Yin, R. (2003). Applications of case study research. 3rd ed.

Devo.com. (2019). Improving the Effectiveness of the Security Operations Center. [online] Available at: https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf [Accessed 1 Jan. 2020].

Cybersecurity.att.com. (2019). 2020 SOC Team (Security Operations Center) Roles | AT&T Cybersecurity. [online] Available at: https://cybersecurity.att.com/resource-center/ebook/building-a-soc/soc-team [Accessed 1 Jan. 2020].

Vijayan, J. (2019). 4 key challenges for next-gen security operations centers | TechBeacon. [online] TechBeacon. Available at: https://techbeacon.com/security/4-key-challenges-next-gen-security-operations-centers [Accessed 5 Jan. 2020].

Ward Solutions. (2019). Five things a Security Operations Center can give you - Ward Solutions. [online] Available at: https://www.ward.ie/five-reasons-you-need-a-security-operations-centre/ [Accessed 3 Jan. 2020].

Panda, P. (2019). 5 Best Practices for Setting Up a Security Operations Center. [online] Appknox.com. Available at: https://www.appknox.com/blog/best-practices-security-operations-center [Accessed 3 Jan. 2020].